Pela boca morre o peixe, e pelo clique a carteira

digitalinside.sapo.pt/pela-boca-morre-o-peixe-e-pelo-clique-a-carteira

Bruno Castro

Se alguém ainda tinha dúvidas de que estamos a viver uma epidemia sistémica de burlas, os últimos casos ocorridos em Portugal oferecem um retrato claro e inquietante de presença constante, invasiva e, muitas vezes, cruel no nosso dia-a-dia. As notícias recentes mostram que as vulnerabilidades humanas estão a ser exploradas com uma eficácia assustadora, e que a sociedade portuguesa ainda não acordou para a dimensão real do problema.

Recentemente, o Ministério Público chamou a atenção para uma burla que circula no WhatsApp, em que mensagens fraudulentas, supostamente da Segurança Social, pressionam os destinatários a fazer pagamentos que não existem. Este tipo de esquema, que se aproveita da confiança que as pessoas têm em instituições públicas e da pressa induzida pelo tom urgente das mensagens, já não é isolado. É um padrão que se repete com pequenas variações em nome de serviços essenciais, públicos e privados.

Foi também notícia recente, casos de extorsão amorosa, em que jovens são enganados emocionalmente após iniciarem contacto em plataformas de encontros online. Depois de uma vídeo chamada íntima, o esquema transforma-se em chantagem: a promessa de mais trocas íntimas converte-se em exigência de dinheiro sob a ameaça de exposição de imagens privadas. Os casos de vítimas emocionalmente vulneráveis e financeiramente expostas, já se multiplicam e as variações continuam.

Burlas de emprego que oferecem trabalho remoto com promessas de ganhos fáceis e que, numa fase posterior, exigem pagamentos (com a promessa de recrutamento ou comissões que nunca chegam), também são alertadas pelo Gabinete de Cibercrime e pelo Ministério Público como esquemas em franca expansão. Este tipo de fraude atinge especialmente jovens e desempregados, isto é, grupos já com fragilidades económicas, explorando a esperança de uma oportunidade que, apenas serve para esvaziar contas bancárias.

Tudo isto decorre num contexto em que o prejuízo causado por burlas em Portugal foi estimado em dezenas de milhões de euros. Embora alguns relatórios mostrem uma diminuição em número de ocorrências recentes, o montante financeiro envolvido continua a ser elevado: mais de 65 milhões de euros em prejuízo patrimonial em 2024, segundo dados da PSP.

O que une estes casos, desde falsas dívidas “urgentes” até extorsões amorosas e promessas de trabalho ilusórias é simples: os burlões jogam com as emoções, confiança e pressa. Sabem como manipular para obter respostas impulsivas: medo de perder direitos, desejo de proximidade emocional, esperança de um ganho fácil. Uma vez que as mensagens chegam de perfis que parecem familiares ou legítimos, muitas pessoas cedem antes de pensar duas vezes. Além disso, também plataformas de IA Generativa auxiliam com a criação e personalização das mensagens para que sejam ainda mais convincentes.

Um elemento que muitas vezes passa despercebido é o *profiling*, ou seja, a análise prévia que os burlões fazem antes de atacar em que recolhem informação pública ou semipública sobre as potenciais vítimas: perfis de redes sociais, gostos, interesses, ocupação, localização, contactos, hábitos de consumo. Com estes dados, conseguem personalizar o golpe, tornando-o mais convincente, credível e emocionalmente manipulador. Em muitos casos, o que leva uma pessoa a cair na burla não é só o conteúdo da mensagem, mas a sensação de que foi feita para ela.

A resposta oficial, com alertas, recomendações para apresentar queixas, avisos através dos órgãos de comunicação social, é necessária, mas insuficiente. As autoridades e plataformas digitais precisam de agir em conjunto, com estruturas eficazes de deteção, bloqueio e responsabilização. As instituições de ensino e a sociedade civil devem transformar a literacia digital em algo essencial para navegar na vida contemporânea. O perigo deixou de ser apenas "clicar no link errado", tornou-se confiar no toque humano, na promessa de amor, no atalho para dinheiro, e isso, só se combate com literacia, medidas técnicas de segurança, e responsabilização máxima.

Bruno Castro é Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense.