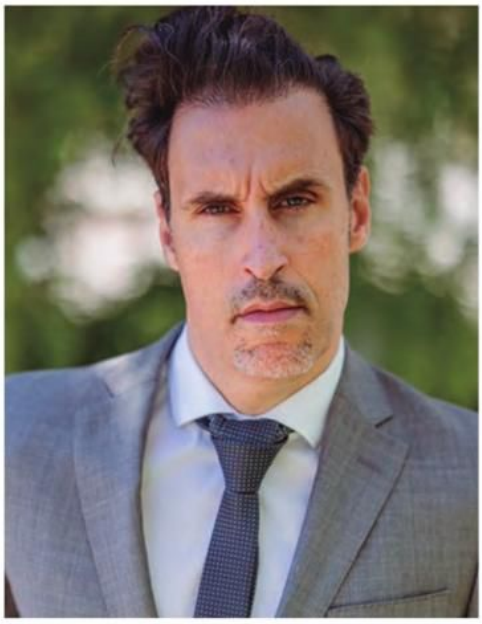

O novo paradigma da segurança digital em pagamentos

Por Bruno Castro,
Fundador e CEO da VisionWare

O setor financeiro está a viver uma transformação profunda com os pagamentos digitais, as transferências instantâneas e as carteiras virtuais a tornaram-se parte do quotidiano de milhões de pessoas e empresas. Esta evolução trouxe conveniência e eficiência, mas também uma nova complexidade inerente, que implica garantir a segurança num ambiente onde a inovação tecnológica aquando da capacidade de a proteger. Num ecossistema cada vez mais digital, a confiança é o verdadeiro capital. E essa confiança depende, acima de tudo, da cibersegurança. O crescimento das fraudes online, das tentativas de phishing e campanhas de engenharia social mostram que a sofisticação dos ataques acompanha o ritmo da inovação. O setor financeiro, pelo seu carácter crítico e pela relevância dos dados e ativos que engloba, é particularmente exposto a riscos de segurança. Além disso, o setor financeiro europeu encontra-se atualmente num período de adaptação e transformação, marcado por uma crescente interdependência entre inovação tecnológica e exigências regulatórias. A União Europeia tem vindo a reforçar a regulação em domínios críticos como os pagamentos digitais, a proteção de dados, a Inteligência Artificial (IA) e a identidade digital. Normas como o Digital Operational Resilience Act (DORA), o AI Act e a futura Third Payment Services Directive PSD3 estabelecem critérios claros de segurança, resiliência e transparência, refletindo a necessidade de conciliar inovação com confiança e proteção do consumidor. Estas regulamentações exigem que as instituições financeiras implementem medidas proativas de gestão de risco digital, auditáveis e capazes de demonstrar conformidade contínua. A conformidade com estes regulamentos não é apenas uma obrigação legal: representa também uma oportunidade estratégica. Instituições que conseguem integrar a segurança, a privacidade e a ética digital nos seus produtos e serviços ganham credibilidade junto de clientes, parceiros e reguladores, reforçando a confiança num setor em que a reputação é um ativo decisivo.

> ***Em Portugal, a Chave Móvel Digital (CMD) é um exemplo notável de autenticação forte e segura, que conjuga um PIN pessoal com um código temporário criado por num dispositivo confiável.***

O PAPEL DA INTELIGÊNCIA ARTIFICIAL

Naturalmente, entre as tecnologias que mais estão a transformar este setor, destaca-se a IA que está a redefinir a forma como as instituições financeiras operam e gerem o risco.

A automatização de processos permite maior eficiência e precisão, reduz custos operacionais, liberta equipas para tarefas de maior valor e, claro, através da capacidade de analisar grandes volumes de dados em tempo real, potencia também uma menor alocação de recursos humanos e tempo.

No domínio da segurança, a IA é também uma aliada poderosa. Os sistemas baseados em aprendizagem automática conseguem identificar padrões anómalos, detetar transações suspeitas e antecipar comportamentos de fraude com uma rapidez impossível de atingir manualmente. A aplicação destas tecnologias contribui para reforçar a proteção de milhões de operações financeiras diárias e para garantir uma maior fiabilidade ao ecossistema de pagamentos.

Contudo, a mesma tecnologia que fortalece a segurança também pode ser utilizada de forma indevida. O desenvolvimento de deepfakes e outras aplicações de IA generativa trouxe um novo tipo de risco e já foram mesmo registadas situações em que vozes e rostos gerados artificialmente foram utilizados para contornar sistemas de autenticação biométrica ou enganar colaboradores e clientes. Estes incidentes mostram que os mecanismos tradicionais de verificação, como a voz, o vídeo ou a imagem, podem ser insuficientes quando confrontados com tecnologias de simulação avançada.

Perante esta realidade, as formas de autenticação mais seguras são aquelas que combinam múltiplos fatores e mecanismos criptográficos, reduzindo o risco de fraude mesmo perante ataques sofisticados.

A autenticação multifatorial (MFA) continua a ser a melhor prática internacional, ao exigir mais de um elemento de validação, algo que o utilizador sabe (por exemplo, uma palavra-passe), algo que possui (um token físico ou dispositivo móvel) e algo que é (biometria).

Em Portugal, a Chave Móvel Digital (CMD) é um exemplo notável de autenticação forte e segura, que conjuga um PIN pessoal com um código temporário criado por num dispositivo confiável. Além de ser um componente forte de segurança, esta solução está integrada em serviços públicos e privados e baseia-se em princípios de segurança criptográfica e identidade verificada.

A CMD e outros mecanismos equivalentes devem servir de referência para o futuro da autenticação em pagamentos digitais, por aliarem simplicidade, fiabilidade e proteção efetiva contra deepfakes e fraudes de identidade.

RECOMENDAÇÕES PARA REFORÇAR A SEGURANÇA DIGITAL NOS PAGAMENTOS

A resposta passa por utilizar a IA de forma responsável, com supervisão humana, transparência e auditorias regulares. A tecnologia deve ser vista como uma extensão da capacidade humana, e não como um substituto da vigilância e da análise crítica. Neste sentido, algumas recomendações importantes a ter em conta são:

- Adotar autenticação multifatorial (MFA): combinar diferentes elementos de verificação (palavra-passe, dispositivo e biometria) para reduzir a probabilidade de acesso indevido;
- Reforçar a identidade digital segura: promover o uso de soluções como a Chave Móvel Digital, que alia praticidade a elevados padrões de segurança;
- Aplicar IA com supervisão e ética: utilizar algoritmos para deteção de fraude e análise comportamental, mas com revisão humana e transparência nos critérios de decisão;
- Apostar na formação e literacia digital: promover a capacitação contínua das equipas. Colaboradores informados conseguem identificar sinais de fraude, manipulação digital ou deepfakes;
- Fomentar a cooperação entre entidades: partilhar informação sobre novas ameaças e boas práticas entre bancos, reguladores e empresas de cibersegurança, criando um ecossistema mais resiliente.

O PAPEL DO UTILIZADOR NA SEGURANÇA DIGITAL

A segurança dos pagamentos digitais não depende apenas da tecnologia. Depende, sobretudo, das pessoas que a utilizam. O utilizador é hoje uma extensão natural dos mecanismos de defesa das instituições financeiras: cada decisão, clique ou confirmação contribui para reforçar, ou comprometer, a segurança de todo o ecossistema.

As instituições devem investir não apenas em ferramentas de proteção, mas também em literacia digital. A sensibilização contínua sobre práticas seguras, autenticação, deteção de fraude e verificação de identidade é tão importante quanto a infraestrutura tecnológica.

Para os utilizadores, isso traduz-se em adotar uma atitude de vigilância digital:

- Confirmar sempre a origem das comunicações e a legitimidade de pedidos de transferência ou atualização de dados;
- Não partilhar códigos, palavras-passe ou dados bancários;
- Evitar o uso de redes ou dispositivos partilhados para operações financeiras;
- Atualizar regularmente software e aplicações;
- Privilegiar canais oficiais e soluções de autenticação segura, como a CMD ou apps bancárias certificadas.

Mais do que uma questão de prudência, trata-se de sermos mais resilientes e compreender que a segurança é uma responsabilidade partilhada.

UMA VISÃO PARA O FUTURO

O futuro dos pagamentos digitais será cada vez mais inteligente, automatizado e integrado. A IA continuará a ser um pilar essencial dessa transformação, mas o equilíbrio entre inovação e segurança será decisivo. Algumas tendências/oportunidades futuras positivas, a meu ver, podem passar pela expansão do uso de chatbots e assistentes virtuais; pelo aumento da automação de tarefas financeiras; o avanço na deteção de fraudes; a personalização de serviços financeiros, direcionadas ao cliente, com base no seu histórico; previsão e análise de mercado mais avançada; e, claro, uma maior ênfase na explicabilidade e ética da IA.

Mas a tecnologia deve evoluir com responsabilidade, acompanhada por regulamentação adequada e por um compromisso ético das organizações que a desenvolvem e aplicam. Na VisionWare, acreditamos que a verdadeira inovação nasce da combinação entre tecnologia, ética e responsabilidade. A cibersegurança não é apenas um requisito técnico: é a base da confiança que sustenta o futuro dos serviços financeiros digitais.**H**