BANCO DE PORTUGAL
EUROSISTEMA

S€PA.PT

Newsletter • N.º 21 • novembro 2022

Editorial

A crescente digitalização da economia tem trazido para a ordem do dia temas como a cibersegurança e a proteção de dados pessoais. O universo dos pagamentos é particularmente afetado por esta evolução, uma vez que os utilizadores recorrem cada vez mais a meios de pagamento eletrónicos, tornando-se alvos preferenciais para infratores que sabem como tirar partido de vulnerabilidades e, assim, contornar os mecanismos de segurança implementados.

Esta *newsletter SEPA.pt* é dedicada ao tema da fraude nos pagamentos, uma realidade muito dinâmica e que exige um acompanhamento próximo dos reguladores e supervisores, prestadores de serviços de pagamento (PSP) e utilizadores.

Os reguladores e supervisores têm estabelecido requisitos mais exigentes de segurança nos pagamentos que estão sujeitos a maior risco de fraude. De entre estes mecanismos, destaca-se a exigência de autenticação forte do cliente em operações de pagamento eletrónicas, introduzida pela Diretiva (UE) 2015/2366, de 25 de novembro, relativa aos serviços de pagamento no mercado interno (Diretiva de Serviços de Pagamento revista ou DSP2).

Para o Banco de Portugal, a prevenção da fraude nos pagamentos é, cada vez mais, uma prioridade.

Os PSP têm, naturalmente, um papel fundamental na promoção da segurança nos pagamentos, por via da implementação de sistemas de deteção e prevenção de fraude e do desenvolvimento de planos de resposta a ataques. São igualmente agentes privilegiados na sensibilização dos utilizadores para os riscos de fraude e para adoção de protocolos que protejam a segurança de comunicações e credenciais.

Não obstante os esforços encetados pelas autoridades e pelos PSP, tem aumentado o recurso a técnicas de fraude que, para contornar os requisitos de segurança mais exigentes, envolvem a manipulação do utilizador. Nestes casos, é ele próprio que acaba por fornecer/comprometer as suas credenciais de segurança ou mesmo por realizar operações em benefício do infrator.

Neste contexto, só uma maior sensibilização e informação dos utilizadores de serviços de pagamento sobre os riscos existentes e sobre os comportamentos a adotar pode diminuir a probabilidade de sucesso das tentativas de fraude, ainda que não a elimine totalmente.

Para reduzir os riscos de fraude, é fundamental que os utilizadores preservem a confidencialidade das suas credenciais de segurança, sejam vigilantes e conheçam os sinais de alerta (como a receção de ofertas "irrecusáveis"), não cliquem em *links* desconhecidos e evitem recorrer a acessos públicos e/ou a computadores partilhados para efetuar pagamento.

Nunca é demais recordar que a segurança nos pagamentos começa em cada um de nós.

Hélder Rosalino
Membro do Conselho de Administração do Banco de Portugal

Fraude nos pagamentos eletrónicos em Portugal

Um mundo cada vez mais digital oferece muitas vantagens aos utilizadores de serviços de pagamento. Graças aos desenvolvimentos tecnológicos, a realização de operações de pagamento é, hoje, mais rápida, fácil e cómoda.

Contudo, esta evolução também traz novos riscos, relacionados, sobretudo, com a suscetibilidade a determinados tipos de fraude, a ciberataques e a incidentes relacionados com as novas tecnologias utilizadas. É importante, por isso, assegurar que os pagamentos eletrónicos são efetuados com respeito pelas regras em vigor e com recurso aos mecanismos de segurança disponíveis.

Acompanhar os níveis de fraude e conhecer os tipos de ataque mais frequentes é fundamental para a respetiva prevenção, seja mediante a introdução de novos mecanismos de prevenção e mitigação, pelos reguladores e pelos próprios PSP, seja pela prestação de informação aos utilizadores, que estarão assim mais aptos a defender-se e a evitar que a fraude se materialize.

Tendências na tipologia de fraude nos pagamentos

A fraude nos pagamentos pode assumir formas muito distintas consoante, por exemplo, quem inicia a operação fraudulenta e qual o método utilizado.

A Autoridade Bancária Europeia (*European Banking Authority* — EBA) distingue, nas Orientações relativas a requisitos de comunicação de dados sobre fraudes nos termos do artigo 96.º, n.º 6, da DSP2, dois tipos de operações a incluir no âmbito do reporte de dados sobre fraude: (i) as **operações de pagamento não autorizadas**, que podem ser efetuadas em resultado da perda, furto ou apropriação indevida de dados de pagamento sensíveis ou de um instrumento de pagamento, ou executadas sem o consentimento do ordenante; e (ii) as **operações de pagamento efetuadas em consequência da manipulação do ordenante** para emitir uma ordem de pagamento ou dar, de boa-fé, instruções nesse sentido ao PSP, para uma conta de pagamento que julga pertencer ao beneficiário legítimo.

No que respeita ao método, existe um vasto conjunto de possibilidades de fraude, algumas das quais têm vindo a tornar-se mais frequentes ou relevantes nos últimos anos, demonstrando que os infratores têm acompanhado os desenvolvimentos tecnológicos e regulamentares. Foi o que aconteceu, por exemplo, nas operações remotas com cartão: as exigências impostas pela regulamentação, com destaque para as regras de autenticação forte do cliente, introduzidas pela DSP2, têm obrigado os infratores a recorrer a novas técnicas.

Neste contexto, são cada vez mais frequentes as situações de fraude decorrentes de **técnicas de engenharia social**, que exploram as vulnerabilidades dos utilizadores de serviços de pagamento, levando-os a executar ações que favorecem o atacante, como, por exemplo, a partilha inadvertida de credenciais de acesso a contas de pagamento.

Consoante o meio através do qual é feito o contacto com a vítima, o ataque pode ser classificado como *phishing* (através de *e-mail*), *smishing* (por SMS) ou *vishing* (através do telefone). Existem também situações em que existe um contacto direto, em pessoa, ou através das redes sociais. Por vezes, os infratores utilizam simultaneamente várias destas técnicas. Estas ações fraudulentas podem ser ainda mais sofisticadas, envolvendo, por exemplo, a realização de contactos telefónicos ou por SMS com replicação do número de telefone do *call center* do PSP (*spoofing*), o que confere maior credibilidade aos contactos efetuados pelo infrator.

Um exemplo de fraude com recurso a engenharia social é a situação em que um utilizador recebe um e-mail, aparentemente remetido pelo seu PSP, no qual é informado sobre a necessidade de efetuar determinada ação (por exemplo, uma atualização de dados pessoais), com um *link* para uma página de internet que replica o *website* do PSP e no qual o utilizador acaba por inserir as suas credenciais de acesso. Posteriormente, o mesmo utilizador recebe uma chamada de alguém que se faz passar por um funcionário da instituição financeira e que lhe solicita elementos adicionais de informação (por exemplo, alegando a existência de operações fraudulentas que é urgente cancelar). Na posse de todos esses elementos, o infrator estará apto a efetuar operações a partir da conta de pagamento do utilizador.

As estratégias em que os infratores se fazem passar por uma outra pessoa (*impersonation scam*) não se restringem aos funcionários dos PSP. Outro exemplo deste tipo de situações, cada vez mais frequente, é aquele em que o infrator se faz passar por um

funcionário superior da empresa a que a vítima pertence, dando-lhe indicações para que seja feita uma transferência urgente para uma conta por ele controlada (*CEO fraud*).

São ainda de realçar os **ataques com *malware***, ou seja, com *software* malicioso que permite atacar organizações ou dispositivos pessoais, e através dos quais o infrator consegue, por exemplo, obter credenciais de acesso a contas de pagamento, ou modificar, a seu favor, ordens de pagamento legítimas.

A relevância da fraude através de *malware* não é recente, mas o aumento da utilização de dispositivos móveis para a realização de pagamentos, nomeadamente através de aplicações de pagamento, tornou estes dispositivos num alvo cada vez mais apetecível para burlões e cibercriminosos. A instalação de *malware* — que ocorre, nomeadamente, quando a vítima acede a um *e-mail* ou *website* corrompido — pode permitir ao infrator apropriar-se de informação armazenada no dispositivo, bem como monitorizar ações que a vítima realize futuramente nesse dispositivo, como a inserção de credenciais de acesso à *app* ou ao *homebanking*.

Estatísticas sobre fraude nos instrumentos de pagamento

No *Relatório dos Sistemas de Pagamentos* relativo a 2021 foram, pela primeira vez, divulgados dados sobre a fraude nos pagamentos em Portugal, respeitantes ao primeiro semestre desse ano. Os dados disponíveis para o segundo semestre de 2021 vêm demonstrar que, apesar do aumento significativo das operações de pagamento eletrónico em Portugal (em detrimento das operações baseadas em papel), os níveis de fraude na utilização dos diferentes instrumentos de pagamento eletrónicos se mantêm muito reduzidos. De facto, embora as operações de pagamento eletrónico tenham aumentado 18% em quantidade e 16% em valor entre o primeiro e o segundo semestre de 2021, as operações fraudulentas diminuíram 25% em quantidade e 12% em valor no mesmo período. No segundo semestre de 2021, foram realizadas cerca de 158 mil operações fraudulentas, num total de aproximadamente 12 milhões de euros, o que corresponde a um valor médio de 75 euros por operação.

Por instrumento, foi nas operações com cartão de pagamento que se registou o maior número de fraudes, seguidas das transferências e dos débitos diretos.

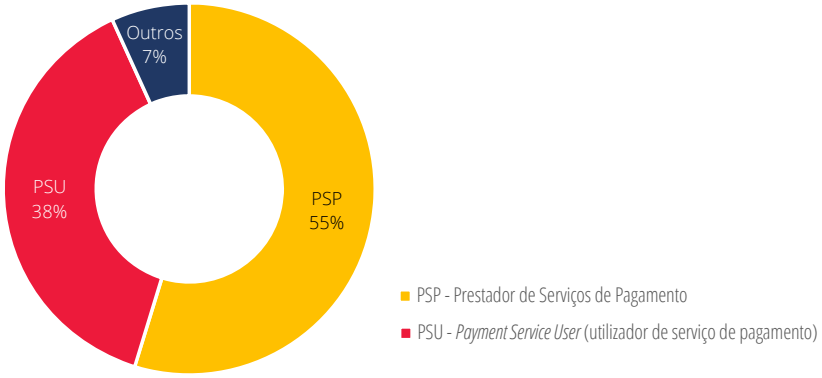
Fonte: Banco de Portugal.

No segundo semestre de 2021, quando comparado com a primeira metade desse mesmo ano, ocorreu uma redução significativa das situações de fraude com débitos diretos e cartões de pagamento, que representaram, respetivamente, 0,0002% e 0,0261% do total de operações realizadas com cada instrumento de pagamento. Pelo contrário, nas transferências a crédito, aumentou o peso das situações de fraude, embora tenha permanecido num nível muito reduzido.

Nas operações com cartão de pagamento em que foi aplicada autenticação forte do cliente, a taxa de fraude foi cerca de seis vezes menor do que a registada nas operações sem esse tipo de autenticação, o que demonstra a eficácia desta medida de segurança.

Note-se que a aplicação de autenticação forte não é obrigatória em todas as operações de pagamento eletrónicas, uma vez que os PSP podem aplicar isenções em determinadas operações (em função do nível de risco envolvido, do montante, da frequência e do canal através do qual a operação é executada). Nestas situações, é o PSP, e não o utilizador, que assume responsabilidade caso a operação de pagamento não seja devidamente autorizada. Este facto justifica que grande parte das perdas decorrentes de operações fraudulentas seja suportada pelos PSP e não pelos utilizadores (Gráfico 1).

Gráfico 1 • Perdas originadas por fraude em operações de pagamento | Segundo semestre de 2021



Fonte: Banco de Portugal.

Ainda que a fraude nos pagamentos eletrónicos em Portugal não assuma níveis que possam ser considerados muito significativos quando comparados com os de outros países europeus, seja em termos absolutos, seja em termos relativos, a prevenção da fraude nos pagamentos tem sido uma prioridade do Banco de Portugal. Nesse sentido, o Banco tem vindo a publicar conteúdos informativos para reforçar a segurança dos utilizadores, nomeadamente, vídeos sobre como podem proteger-se da fraude *online* e sobre autenticação forte do cliente, bem como boas práticas a observar na utilização de cartões e na realização de pagamentos na *internet*.

Acontecimentos relevantes

- Reunião do Fórum com a Indústria para a Cibersegurança e Resiliência Operacional, 15 de dezembro de 2021;
- Publicação, pela Autoridade Bancária Europeia (EBA), do Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, 18 de janeiro;
- Publicação do estudo do Parlamento Europeu *The digital euro: policy implications and perspectives*, 21 de janeiro;
- Divulgação, pelo Banco de Portugal, de Boas práticas de débitos diretos para entidades credoras, 25 de janeiro;
- Atualização da página web dedicada à evolução da Estratégia Nacional para os Pagamentos de Retalho | Horizonte 2022, com referência ao 4.º trimestre 2021, 2 de fevereiro;
- Reunião do European Forum for Innovation in Payments (EFIP), 9 de fevereiro;
- Publicação do *Relatório de Atividades da Subcomissão Especializada para a Área de Inovação Digital e Fintech (SCTECH)* referente a 2020-2021, 16 de fevereiro;
- Comunicado sobre como a pandemia alterou os hábitos de pagamento em Portugal em 2021, 23 de fevereiro;
- Publicação, pela EBA, de Orientações sobre a exclusão relativa a redes restritas ao abrigo da Diretiva de Serviços de Pagamento 2 (DSP2), 24 de fevereiro;
- Divulgação de *podcast* "O que deve saber sobre o seu cartão de pagamento", 3 de março;
- Reunião interbancária sobre sistemas de pagamentos, 17 de março;
- Lançamento de consulta pública da Comissão Europeia sobre o euro digital, 5 de abril;
- Publicação, pela EBA, do *Final Report on amending RTS on SCA and CSC under PSD2*, 5 de abril;
- Divulgação de *podcast* sobre 20 anos do euro — passado, presente e futuro da moeda única, 7 de abril;
- Publicação do *Relatório de Atividades do Fórum para os Sistemas de Pagamentos* referente a 2021, 8 de abril;
- 1.ª reunião do Grupo de Contacto do Banco de Portugal com o Mercado sobre o Euro Digital, 21 de abril;
- Lançamento, pelo Banco Central Europeu, de pedido de manifestações de interesse em participar num exercício de desenvolvimento de protótipos de interfaces com os utilizadores para pagamentos em euro digital, 28 de abril;
- Divulgação de *podcast* sobre a evolução do mercado de pagamentos, 28 de abril;
- Publicação do *Relatório dos Sistemas de Pagamentos* referente a 2021, 29 de abril;
- Evento "Como proteger os pagamentos? (Ciber)Segurança e prevenção da fraude", 2 de maio;
- Publicação do *Relatório de Atividades do Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO)* referente a 2021, 3 de maio;

- Comunicado do Banco de Portugal sobre a publicação do quadro de referência TIBER-PT, para realização de testes de cibersegurança avançados por bancos portugueses, 3 de maio;
- Lançamento de consulta da Comissão Europeia sobre a revisão da DSP2, 10 de maio;
- Acordo provisório entre a Presidência do Conselho da União Europeia e o Parlamento Europeu sobre o Regulamento de Resiliência Operacional Digital (DORA), 10 de maio;
- Atualização da página *web* dedicada à evolução da Estratégia Nacional para os Pagamentos de Retalho | Horizonte 2022, com referência ao 1.º trimestre de 2022, 12 de maio;
- Lançamento da 4.ª edição do Portugal Finlab e publicação do relatório da 3.ª edição do Portugal Finlab, 17 de maio;
- Publicação do estudo do Banco Central Europeu *Costs of retail payments – an overview of recent national studies in Europe*, 20 de maio;
- Lançamento, pelo European Payments Council (EPC), de *consulta pública relativa ao rulebook do SEPA Payment Account Access scheme*, 13 de junho;
- Publicação, pela EBA, da resposta ao *call of advice* da Comissão Europeia sobre a revisão da PSD2, 23 de junho;
- 2.ª reunião do Grupo de Contacto do Banco de Portugal com o Mercado sobre o Euro Digital, 24 de junho;
- Acordo provisório entre a Presidência do Conselho da União Europeia e o Parlamento Europeu sobre o Regulamento Mercados de Criptoativos europeu (MiCA), 30 de junho;
- Reunião plenária do Fórum para os Sistemas de Pagamentos, 1 de julho;
- Reunião do Euro Retail Payments Board (ERPB), 7 de julho;
- Publicação, pelo Banco Central Europeu, das *Payments statistics*: 2021, 22 de julho;
- Atualização da página *web* dedicada à evolução da Estratégia Nacional para os Pagamentos de Retalho | Horizonte 2022, com referência ao 2.º trimestre 2022, 25 de julho;
- Publicação, pelo Banco Central Europeu, de documento "The case for a digital euro: key objectives and design considerations", julho de 2022;
- Publicação de estudo do Banco Central Europeu *Towards the holy grail of cross-border payments*, agosto;
- Anúncio, pelo Banco Central Europeu, das entidades selecionadas para o desenvolvimento de interfaces com os utilizadores para pagamentos em euro digital, 16 de setembro;
- Seminário do Fórum para os Sistemas de Pagamentos sobre o euro digital, 29 de setembro;
- Publicação, pelo Banco Central Europeu, de documento sobre o progresso da fase de investigação do projeto do euro digital, 29 de setembro;
- Campanha dos 20 anos do euro no LinkedIn e Instagram: "O papel? Qual papel?", "Esperar é tão 2017", "Clique e siga", "Boas notícias para os mais esquecidos", "Uma forma ainda mais segura de pagar", "Sabia que há mais de 700 em Portugal?" e "Consultar informação das suas contas, num só local?", setembro;
- Reunião do Fórum com a Indústria para a Cibersegurança e Resiliência Operacional, 3 de outubro;
- Publicação do vídeo "As "moedas virtuais" não são verdadeiras moedas. Saiba porquê", 3 de outubro;
- Publicação do vídeo "O Euro digital e os criptoativos. Que diferenças?", 6 de outubro;
- Publicação do vídeo "Sabia que ao investir em ativos virtuais está a fazê-lo por sua conta e risco?", 7 de outubro;
- Lançamento, pelo Banco Central Europeu, de concurso para a contratação de um *scheme rulebook manager* para o euro digital, 10 de outubro;
- Lançamento de consulta pública do Banco de Portugal n.º 8/2022, sobre a abordagem estratégica do Banco de Portugal aos facilitadores de inovação, 21 de outubro;
- 3.ª reunião do Grupo de Contacto do Banco de Portugal com o Mercado sobre o Euro Digital, 24 de outubro.
- Proposta legislativa da Comissão Europeia sobre transferências imediatas, 26 de outubro;
- Atualização da página *web* dedicada à evolução da Estratégia Nacional para os Pagamentos de Retalho | Horizonte 2022, com referência ao 3.º trimestre 2022, 26 de outubro;
- Reunião interbancária sobre sistemas de pagamentos, 7 de novembro de 2022;
- Conferência conjunta Banco Central Europeu/Comissão Europeia "Towards a legislative framework for a digital Euro", 7 de novembro.

Newsletter SEPA.pt • Banco de Portugal Av. Almirante Reis, 71 | 1150-012 Lisboa • www.bportugal.pt • Edição Departamento de Sistemas de Pagamentos | Área de Inovação e Políticas de Pagamentos • *Design* Departamento de Comunicação e Museu | Unidade de *Design* • ISSN 2182-2816 (*online*)