QUICKCLICK

CARTA CIRCULAR DO BANCO DE PORTUGAL

TRATAMENTO PRUDENCIAL PHISHING

SPS
SOCIEDADE DE ADVOGADOS
DO SEU LADO
desde 1989

CARTA CIRCULAR DO BANCO DE PORTUGAL

TRATAMENTO PRUDENCIAL PHISHING

SPS SOCIEDADE DE ADVOGADOS
DO SEU LADO desde 1989

QUICKCLICK

Carta Circular n.º CC/2023/00000025

No passado dia 21 de Junho de 2023 o Banco de Portugal publicou a **Carta Circular n.º CC/2023/00000025**, através da qual se transmite um **conjunto de recomendações com vista a assegurar a minimização dos impactos associados a eventos de phishing sobre clientes**.

Considerando **I)** a crescente digitalização das atividades de serviços financeiros e que **II)** o Phishing tem vindo a assumir uma relevância crescente, entende o Banco de Portugal que é essencial que as instituições assegurem uma gestão adequada dos riscos a que se encontram expostas.

Nesse sentido, e através da presente Carta Circular, o Banco de Portugal transmite às instituições de crédito, instituições de pagamento e instituições de moeda eletrónica com sede em Portugal, e às sucursais de instituições destes tipos, autorizadas a exercer atividade em Portugal com sede em países que não sejam Estados-Membros da União Europeia, as seguintes **recomendações:**

Deveres de comunicação

A ocorrência de situações de burla, de fraude, ou de natureza similar, com recurso a técnicas de phishing, em contas de titulares junto das instituições ("incidentes de phishing"), constitui: i) **um incidente de cibersegurança**, na aceção da alínea c) do n.º 2 do artigo 1.º da Instrução n.º 21/2019 do Banco de Portugal; e ii) um **incidente de segurança,** no âmbito da Instrução n.º 1/2019 do Banco de Portugal.
Assim, as **instituições devem assegurar o cumprimento, de forma diligente, proativa e tempestiva, dos deveres de informação** perante as demais autoridades competentes da ocorrência destes incidentes, nomeadamente do foro judicial, de proteção de dados ou da cibersegurança, com vista à eficaz resolução dos incidentes e para mitigação do potencial impacto sistémico, por contágio, de incidentes.

Para a avaliação dos critérios aplicáveis para o dever de reporte, **as instituições devem considerar a série de eventos**, e não os eventos individuais, **quando exista evidência de que estão relacionados**; adicionalmente, as instituições devem ainda observar sempre o disposto no n.º 11 do artigo 4.º da Instrução n.º 21/2019, bem como o disposto no n.º 8.3 e no n.º 8.5 da Instrução n.º 1/2019.

Quadro de gestão de riscos

A ocorrência de incidentes de phishing constitui um **indício de potenciais insuficiências no quadro de gestão do risco operacional das instituições,** pelo que deve ser alvo de registo, monitorização, avaliação e atuação pelas funções de controlo interno, em particular pela função de gestão de riscos; é realçada a necessidade de observância das Orientações relativas à gestão do risco associado às tecnologias de informação e comunicação e à segurança (EBA/GL/2019/044).

Perdas operacionais

As instituições devem **registar estes incidentes na sua base de dados de eventos de perda de risco operacional**, e fundamentar devidamente a decisão sempre que entendam não registar uma perda operacional associada no caso de incidentes significativos de phishing dirigidos a clientes, nomeadamente por constituir um **indício de potencial perda futura decorrente**, por exemplo, da obrigação de ressarcir os clientes por instauração de processo judicial por estes junto dos órgãos competentes.
Para o efeito, as Instituições deverão ter em conta **I)** as regras contabilísticas aplicáveis, em cumprimento do Aviso n.º 5/2015 do Banco de Portugal; **II)** das obrigações de reporte para efeitos de supervisão, designadamente as previstas no Regulamento de Execução (UE) 2021/451 da Comissão; e **III)** requisitos em matéria de autoavaliação do capital interno, incluindo em termos reputacionais (conforme previsto no artigo 115.º-J do RGICSF e na Instrução n.º 3/2019 do Banco de Portugal).