Ce

Comunicações electrónicas

Procedimento de Prevenção e Combate a esquemas de fraudes a consumidores (StopFraudes)

Contacte a nossa equipa:

Luís Salvador Pisco
comunicacoes@deco.pt

DECO

Associação Portuguesa para a Defesa do Consumidor

Prevenção e Combate a esquemas de fraudes a consumidores (StopFraudes)

PROBLEMAS E SOLUÇÕES

DECO
SEMPRE CONSIGO

Voz dos Consumidores

' ïňţě' ěĂ

Vivemos numa sociedade cada vez mais digital. E se uma economia mais digital trouxe enormes benefícios para os consumidores, a verdade é que gerou também novos desafios quanto à proteção de direitos e necessidade de prevenção da prática de crimes através de meios digitais, como a violação da privacidade, utilização abusiva de dados pessoais, hackeamento de contas, furtos de identidade, burlas, práticas de *phishing*, *smishing* e *vishing*, muitas vezes com recurso a outras técnicas como o *pharming* e *spoofing,* etc. Com efeito, o recurso a novas tecnologias e a IA, permitiu aos *scammers*[1] (burlões) aceder a um número crescente de consumidores. A mesma tecnologia que nos permite conectar com a família e amigos, permite aos *scammers* e organizações criminosas aceder facilmente aos consumidores, em suas casas.

Nos últimos meses, temos assistido em Portugal a um número cada vez maior de tentativas de burla e de fraudes em geral, dirigidas aos consumidores, através de anúncios fraudulentos em plataformas digitais sobre serviços e produtos financeiros, por exemplo, através de SMS *(smishing)* e de insistentes chamadas de voz *(vishing)*, para os números pessoais dos portugueses, através dos quais se explora a confiança, a ingenuidade e iliteracia digital dos consumidores, fazendo-se passar por entidades confiáveis, para pressionar as vítimas a aceder a links maliciosos, a fornecer dados pessoais e bancários, ou mesmo a convencê-los a fazer pagamentos a favor dos criminosos.

Porque é preciso?

Quase todos nós já fomos alvos de tentativas de *scams* através de chamadas telefónicas, como, por exemplo:

- chamadas de números desconhecidos que, se o consumidor atender, ouve uma voz gravada a informar que receberam o seu currículo e estão interessados em combinar uma entrevista para um emprego, mas que para isso precisam de dados (ou mesmo de um pagamento) do consumidor;

[1] A opção pela utilização neste documento dos substantivos "*Scam*" e *"Scammer"* da língua inglesa é intencional, uma vez serem estas as designações comummente utilizadas em todas línguas, países e continentes, para descrever estas tentativas de burla e quem as pratica.

- chamadas em que afirmam tratar-se do banco do consumidor, por existir um problema com a conta bancária e ser necessária uma confirmação urgente de dados bancários ou fazer uma transferência, sob pena da conta ser bloqueada;
- chamadas de entidades de serviços de pagamentos online, afirmando terem valores para depositar a favor do consumidor, pelo que necessitam de confirmar os seus dados bancários;
- chamadas de alguém que se faz passar por um mediador financeiro que apresenta um negócio de enriquecimento rápido, mas, por se tratar de uma oportunidade única, terá de ser feito um pagamento imediato pelo consumidor.

O mesmo acontece no serviço de mensagens (SMS) ou de mensagens instantâneas em aplicações de redes sociais, através do qual recebemos mensagens que pretendem levar ao engano o consumidor e levá-lo a fazer pagamentos ou a aceder a links maliciosos, como, por exemplo:

- SMS de supostos serviços de entregas, ainda que o consumidor não espere nenhuma encomenda;
- fazendo passar-se por um familiar próximo (como no *scam* do *"olá Pai/olá Mãe"*) que precisa urgentemente de dinheiro, indicando uma referência MB Way para o efeito;
- fazendo passar-se por entidades idóneas como o Serviço Nacional de Saúde (SNS) ou Autoridade Tributária (AT), a cobrar com urgência uma dívida inexistente e fornecendo a entidade/referência/valor para pagamento no Multibanco;
- muitas destas SMS são acompanhadas de *links* maliciosos que, se carregados, permitem ao *scammer* o acesso a dados sensíveis dos telefones dos consumidores *(pharming)* ou os direcionam para websites mascarados *(spoofing com pharming)*, transmitindo uma sensação de aparente segurança e normalidade, para, então aí, ser aplicado o golpe, através de furto de dados ou forçado um pagamento.

Embora muitas empresas possuam já nos seus websites alguma informação dirigida aos seus clientes, sobre os *scams* mais recentes que envolvem o seu nome e sobre quais as tendências de tentativas de fraude com recurso ao serviço que prestam, a verdade é que essa informação é, muitas das vezes, vaga, dispersa e insuficiente, estando os consumidores por sua conta e risco contra as inúmeras formas de novas burlas.

Ora, entendemos que o combate destes esquemas/práticas fraudulentas implica, necessariamente, um papel mais ativo e interessado por parte das empresas que prestam determinados serviços.

Em que consiste o procedimento StopFraudes?

I. Obrigações de prevenção, deteção e repressão:

1. O procedimento StopFraudes consiste no estabelecimento de um conjunto de obrigações e assunção de medidas, a introduzir por via legislativa[2], a cumprir pelas empresas cujos serviços estejam incluídos no seu âmbito de aplicação e que correspondem a setores de atividade nos quais os *scammers* operam prioritariamente.

À semelhança das melhores práticas conhecidas[3], propõe-se que os setores de atividade a incluir inicialmente neste procedimento, sejam a Banca (instituições bancárias e outras instituições de pagamento), as Telco (empresas prestadoras de serviços de comunicações eletrónicas) e os prestadores de serviços intermediários, como as redes sociais, motores de busca, outras plataformas digitais e mercados em linha, que disponibilizem ou possam disponibilizar um serviço de mensagens instantâneas. Sem prejuízo disso, este procedimento deve ser ativamente dinâmico, de forma a vir a incluir, futuramente, se e quando necessário, novas ameaças e setores.

É definido um conjunto de obrigações de prevenção, deteção e repressão destas práticas fraudulentas, aplicáveis às empresas dos setores abrangidos, que torna obrigatória a implementação de medidas técnicas, prudenciais e outras, adequadas a mitigar e combater a ocorrência destas práticas. Igualmente, é estabelecido um regime de compensação, a favor dos consumidores lesados, quando ocorra o seu incumprimento.

A lei deve ainda prever um "Código de Conduta", no qual serão estabelecidas regras de agilização das comunicações entre as entidades e a própria execução prática das obrigações decorrentes das normas legais, vinculando todas as empresas dos setores abrangidos. Pode este código de conduta ser ainda alargado a associações representativas da Banca (ex: Associação Portuguesa de Bancos), associações representativas das Telco (ex: Apritel e Apdc), eventuais representantes dos prestadores de serviços intermediários, reguladores dos setores (ANACOM e Banco de Portugal) e associações de consumidores (como a DECO).

E que obrigações são estas?

---

[2] Como no caso do SPF australiano, que foi introduzido num capítulo da lei da concorrência destinado à proteção dos utilizadores dos serviços aí regulados.
[3] Como são o caso do *"Scams Prevention Framework"* australiano, o *StopScamUK*, do Reino Unido, ou o *"ScamShield"* de Singapura.

2. **Obrigações de prevenção:**

As empresas ficam obrigadas a tomar as medidas, técnicas, prudenciais e outras, que sejam necessárias e adequadas a razoavelmente prevenir que estas práticas de burlas e outras fraudes cheguem aos seus clientes/consumidores.

A título de mero exemplo, indicam-se algumas medidas possíveis:

Banca:

- avisos proativos aos clientes, relativos a tentativas de fraudes recentes ou tendências.
- Implementação de mecanismos ou ferramentas de monitorização de transações padrão, suspendendo uma transação suspeita até obter confirmação do consumidor/utilizador.

Telco:

- Registo de *IDS (intrusion detection system)* de remetentes de SMS, para prevenir que *Scammers* se façam passar por uma entidade, marca ou serviço idóneo.
- Utilização do *SMS Sender ID Registry (SSIR)*, que permite às empresas identificar as não registadas e informar os clientes destinatários dessas mensagens de texto como *"Likely SCAM"*.
- Implementação de *"in-network scanning solutions"* que permite o bloqueio de *Scams* SMS antes que cheguem aos destinatários (consumidores).
- Bloqueio de *Robocalls (Pattern Recognition Technology).*

Plataformas digitais:

- Bloqueio de posts de publicidade a esquemas financeiros fraudulentos (como, por exemplo, os que utilizam falsamente celebridades).

Algumas das obrigações de prevenção já decorrem de diplomas legais, como é o caso do Regulamento dos Serviços Digitais (DSA)[4] relativamente às plataformas digitais, mas que podem ser reforçadas ou regulamentadas neste procedimento.

Do mesmo modo, quanto às entidades bancárias, algumas das obrigações a incluir no procedimento podem vir a resultar, entretanto, da futura Diretiva e do Regulamento dos Serviços de Pagamento (PSD3/PSR). A expetativa é de que haja um conjunto de obrigações sobre as

[4] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE.

entidades de pagamento, em que se incluem os bancos, na deteção, prevenção e tratamento/reembolso de casos de fraudes e burlas. Seja como for, tais obrigações podem vir a ser eventualmente melhoradas no procedimento.

3. **Obrigações de deteção e repressão:**

As empresas ficam obrigadas a tomar ativamente todas as medidas razoáveis para detetar fraudes/tentativas de burla enquanto ocorrem ou imediatamente após ocorrerem. Para este efeito, deve considerar-se como "medidas razoáveis" as que sejam mais práticas, apropriadas e proporcionais, em função da ameaça, não devendo existir uma solução *"one size fits all"*.

Para efeito do estabelecimento de obrigações de deteção e repressão, podem ainda aqui ser adotadas (com a devida adaptação) as obrigações relativas à promoção de solidez, exatidão e cibersegurança, estatuídas nos artigos 15.º, 16.º e 17.º do Regulamento da Inteligência Artificial[5]. Igualmente, para efeitos de controlo e avaliação de riscos, podem aqui ser adotadas (com a devida adaptação) as obrigações estatuídas nos artigos 34.º e 35.º do DSA e, para efeitos de segurança, as dos artigos 32.º a 35.º do Regulamento Geral de Proteção de Dados (RGPD)[6].

A título de mero exemplo, indicam-se algumas medidas possíveis:

Banca:

- Envio de avisos aos clientes, em tempo real, para certos tipos de pagamentos considerados de maior risco.
- Adoção de tecnologia e controlo para prevenção de fraude de identidade, incluindo biométrica, para novos clientes que abram contas online.
- Disponibilização de um canal de denúncias 24/7 para os consumidores reportarem suspeitas de atividades ilícitas.
- Envio de alertas, em tempo real, quando for ativado uma password de uso único.

Telco:

- Implementação de um filtro *anti-scam* de bloqueio de mensagens SMS que contenham links conhecidos de *phishing* ou outro tipo malicioso.
- Investigar e tomar as medidas razoáveis de bloqueio de chamadas fraudulentas originadas na sua rede.

[5] Regulamento (UE) 2024/1689 do Parlamento e do Conselho, de 13 de junho de 2024.
[6] Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016.

- Implementação de processos e algoritmos de monitorização de chamadas de voz e mensagens fraudulentas, com indicadores específicos como o volume alto, atividade de curta duração e utilização de URLs maliciosos nos textos[7].
- Informar os consumidores no seu website sobre potenciais esquemas de fraude de que podem vir a ser vítimas.
- Adotar procedimentos de cooperação com outras operadoras de comunicações par rastrear a origem das chamadas suspeitas de ser fraudulentas.

Plataformas digitais:

- Utilização de algoritmos para deteção de potenciais fraudes.
- Adoção de medidas de verificação de novas contas.
- Verificação se os anunciantes de produtos financeiros estão autorizados para esse efeito pela legislação portuguesa.
- Tomar medidas técnicas de deteção de contas e anúncios fraudulentos.
- Disponibilizar sítio com informação centralizada sobre as medidas tomadas pela plataforma para proteger os utilizadores e medidas que estes devem adotar.
- Suspender e bloquear contas suspeitas de atividades fraudulentas.
- Remover conteúdos associados a atividades fraudulentas.

II. Âmbito de aplicação:

Que fraudes cabem no âmbito do procedimento?

Este procedimento pretende ser prático, eficaz e rápido, com o objetivo de prevenir, detetar e reprimir apenas aquelas *scams* executadas com recurso a serviços de comunicações eletrónicas (como chamadas de voz, serviços de mensagens ou prestadores de serviços intermediários), das quais, em sua consequência, podem ocorrer pagamentos a favor do *scammer* e/ou o fornecimento de dados pessoais do consumidor.

Por esse facto, o seu âmbito aplica-se exclusivamente a:

[7] O artigo 53.º, n.º 5 da Lei das Comunicações Eletrónicas (Lei n.º 16/2022, de 16 de Agosto, na sua versão atual), que transpôs o artigo 97.º, n.º 2 do Código Europeu das Comunicações Eletrónicas (Código Europeu das Comunicações Eletrónicas (aprovado pela Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro), já atribui competência à ANACOM para ordenar aos fornecedores de redes públicas de comunicações ou de serviços de comunicações eletrónicas, o bloqueio, caso a caso, do acesso a números e serviços, sempre que tal se justifique por motivos de fraude ou utilização abusiva.

- Tentativas de levar um consumidor a fazer um pagamento/transferência a favor de um *scammer*, usando um ou mais serviços abrangidos pelo procedimento, como, por exemplo, uma chamada de voz ou um serviço de mensagens.
- Tentativas de enganar um consumidor, levando-o a fornecer dados bancários, senhas ou outros dados pessoais a um *scammer*, usando um serviço abrangido pelo procedimento, como, por exemplo, um esquema de *smishing* numa aplicação de mensagens.
- Estão incluídos no âmbito deste procedimento todas as modalidades de *phishing*, como o *smishing* e o *vishing* que sejam utilizados num *scam* dirigido a um consumidor, com ou sem recurso a outras técnicas como, entre outras, o *spoofing* ou o *pharming*.

O que fica de fora do procedimento?

- O Cibercrime em geral, com exceção do *phishing* e suas variantes de *smishing* e *vishing*, (com ou sem recurso a técnicas como o *pharming* e *spoofing*), enquanto técnicas de engenharia social que utilizam chamadas telefónicas e serviços de mensagens para enganar as vítimas e obter informações confidenciais, como dados bancários, senhas ou outros dados pessoais.
- O comércio eletrónico em geral, a menos que o *scam* tenha como objeto o engano sobre uma inexistente compra e venda de bens e seja realizado com recurso a serviços de comunicações eletrónicas ou plataformas digitais;
- Práticas de crimes sob ameaça presencial, como o roubo;
- Fraudes em que não exista qualquer ação praticada pelo consumidor ou interação deste com o *scammer*.

III. Contacto único:

Este procedimento deve permitir um mecanismo de contacto único, funcionando em regime de *one-stop shop*, ou seja, o consumidor que seja vítima de um *scam* pode opcionalmente contactar a sua operadora, banco ou plataforma, expondo a situação de que foi vítima, independentemente de ser essa a entidade mais indicada para o fazer. A empresa que recebeu a denúncia e recolheu os dados da reclamação, deve tratar a reclamação ou reencaminhá-la para a empresa mais adequada (por exemplo, o consumidor denuncia à sua operadora de comunicações ter sido enganado e realizado um pagamento por transferência da sua conta no Banco X. A operadora deve dar conhecimento imediato da situação a esse banco).

IV. Centro Antifraude:

De forma a tornar mais ágil a prevenção e deteção de autores de fraudes, deverá ser equacionada a criação de um “Centro Antifraude”, cuja função seria a de centralizar, organizar, monitorizar e disseminar toda a informação entre empresas, funcionando ainda como parceiro

dos reguladores, autoridades de aplicação da lei e consumidores. A centralização de toda a informação neste órgão permitiria disseminar a informação a outras empresas, órgão de polícia criminal, ministério público, dando maior eficácia e agilidade às medidas de prevenção, deteção e repressão de atividades fraudulentas.

Pelas suas especiais competências na área da cibersegurança, o Centro Nacional de Cibersegurança (CNCS) deve participar neste Centro Antifraude.

V. Compensação aos consumidores por danos:

O incumprimento das obrigações por parte das empresas deve dar lugar à responsabilização destas perante os consumidores, pelos danos causados. Nesse sentido, deve ser estabelecido um regime simples e célere de ressarcimento dos consumidores pelos danos sofridos diretamente do incumprimento de obrigações decorrentes do procedimento e impostas às empresas.

VI. Linha Telefónica Antifraude:

À semelhança do que acontece no Reino Unido[8], deverá ser criada uma linha telefónica dedicada, de três algarismos (Tipo 222) para os consumidores que foram ou estejam a ser abordados por um *Scammer.*

Este número funcionaria da mesma forma que o 112, permitindo ao consumidor falar imediatamente com a sua operadora de comunicações ou o seu banco, qualquer que ele seja, reportar o sucedido e encontrar auxílio.

No caso de ser adotada esta medida, poderá esta linha funcionar como o contacto único *(one-stop shop)* suprarreferido, que deve ser ampla e publicamente divulgada entre os cidadãos, permitindo uma utilização fácil e forma segura dos cidadãos partilharem as burlas ou tentativas de que foram alvo. Esta linha pode ser gerida por uma associação de consumidores e em colaboração com o Centro Antifraude.

VII. Mecanismo de resolução de conflitos:

Deverá ainda ser prevista a obrigação das empresas abrangidas possuírem um mecanismo interno de resolução de conflitos para lidar com as reclamações dos consumidores. No caso de

[8] *Stop Scams UK Call 159*.

este mecanismo não conseguir resolver o conflito entre consumidor e a empresa, o primeiro poderá apresentar a sua reclamação junto de um Centro de Arbitragem de Conflitos de Consumo.

DECO

SEMPRE CONSIGO

deco.pt

CONTACTE-NOS:

DECO LISBOA (SEDE)
R. de Artilharia Um, nº 79, 4.º
1269-160 Lisboa
Tel.: 21 371 02 00
deco@deco.pt

DECO DELEGAÇÕES

DECO MINHO
Av. Batalhão Caçadores 9,
nº 279 4900-341 Viana do Castelo
Tel.: 258 821 083
deco.minho@deco.pt

DECO NORTE
R. da Torrinha, n.º 228 H, 5.º
4050-610 Porto
Tel.: 223 391 960
deco.norte@deco.pt

DECO CENTRO
R. Padre Estevão Cabral,
n.º 79, 5.º, Sala 504
3000-317 Coimbra
Tel.: 239 841 004
deco.centro@deco.pt

DECO RIBATEJO E OESTE
R. Eng. António José Souto
Barreiros Mota, nº 6 L
Tel.: 243 329 950
deco.ribatejoeoeste@deco.pt

DECO ALENTEJO
Travessa Lopo Serrão,
n.º 15A e 15B, r/c
7000-629 Évora
Tel.: 266 744 564
deco.alentejo@deco.pt

DECO ALGARVE
R. Dr. Coelho de Carvalho, n.º 1 C
8000-322 Faro
Tel.: 289 863 103
deco.algarve@deco.pt

DECO MADEIRA
Loja do Munícipe do Caniço
Rua Doutor Francisco Peres
9125-014 Caniço
Tel: 968 800 489
deco.madeira@deco.pt

fale connosco

966 449 110