Aliança para
a Cibersegurança

Medidas de proteção contra Fraudes por *Spoofing* nas comunicações

O "*spoofing*" por impersonificação é um tipo de ataque malicioso, onde o criminoso assume a identidade de uma origem fidedigna, com o propósito de obter informações confidenciais, credenciais de acesso, ou na persuasão da vítima para a execução de ações que favoreçam o atacante, tais como transferências monetárias ou a instalação de programas informáticos maliciosos.

Estes ataques podem ocorrer por diversas vias, incluindo através da realização de chamadas telefónicas ou de envio de mensagens SMS em que os atacantes simulam a identidade de empresas ou serviços públicos nacionais legítimos.

Para combater este fenómeno, parte significativa dos países europeus[1] têm vindo a implementar medidas regulatórias e técnicas que visam mitigar estes ataques que comprometem **a integridade das telecomunicações** nacionais.

Portugal, é um dos poucos países da Europa que **ainda não implementou qualquer medida técnica para limitar a ação dos Ciber-criminosos nas fraudes através de *spoofing***. É crucial que o país não fique para trás nesta matéria, pois a falta de ações concretas torna-o num alvo privilegiado para estes atores maliciosos.

O *spoofing* provoca impactos expressivos não apenas para os cidadãos, vítimas destas fraudes, como para as entidades impersonificadas, que sofrem prejuízos financeiros significativos, impactos operacionais[2] e danos na reputação junto dos seus clientes e do público em geral, mas também para as autoridades judiciais, que são obrigadas a investir tempo e recursos substanciais no apoio às vítimas e na investigação destes incidentes.

A Aliança para a Cibersegurança, alinhada com a sua missão de **promover uma cultura nacional de Cibersegurança** e um **ciberespaço nacional mais seguro e resiliente,** e cujos membros se encontram diariamente na linha da frente no combate a este fenómeno, vem, deste modo, **reforçar a importância de que as autoridades responsáveis pela segurança das comunicações nacionais, assegurem, com sentido de urgência, um enquadramento**

[1] Entre os quais a Alemanha, Bélgica, Espanha, Finlândia, França, Irlanda, Itália, Malta, Reino Unido, República Checa, Polónia e Suécia

[2] Que resultam de picos de chamadas nos *contact centres* e canalização de meios e recursos para a realização de desmentidos e alertas públicos.

regulatório que permita a implementação das medidas técnicas necessárias para mitigação deste fenómeno.

Com o objetivo de contribuir para uma discussão mais informada sobre o tema, elencamos, em Anexo, algumas medidas técnicas que foram adoptadas por outros países europeus com sucesso, e cuja adoção pode ser equacionada em Portugal.

Lisboa, 10 de Dezembro de 2025,

Os Membros da Aliança para a Cibersegurança

ANEXO - Medidas adotadas nos restantes países Europeus

Fonte: Cullen Internacional

1. **Bloqueio de chamadas internacionais com o identificador de chamada "*Calling Line Identification*" (CLI) nacional**

Os operadores de telecomunicações implementam mecanismos de bloqueio para chamadas originadas no estrangeiro que utilizem um número nacional como identificador de chamada (CLI).

O bloqueio de números fixos é, de forma geral, mais comum, embora possam existir exceções previstas pela regulamentação nacional.

Adicionalmente, algumas jurisdições exigem também o bloqueio de números móveis, assegurando simultaneamente que os utilizadores legítimos em situação de roaming não sejam indevidamente afetados por estas restrições.

Países que adotaram esta medida: Bélgica, Espanha, Finlândia, Irlanda, Itália, Malta, Polónia, Suécia e Reino Unido.

2. **Registo de identificadores e remetente de SMS**

É criada, mantida e atualizada uma base de dados nacional de remetentes alfanuméricos SMS autorizados, bem como os respetivos sistemas de onde mensagens SMS podem ser enviadas para cada respetivo remetente.

Esta base de dados é utilizada por todos os operadores, para validar se um determinado remente de um SMS está na lista, e se foi enviado a partir de um sistema autorizado, devendo os operadores bloquear os SMS cujo identificador não esteja registado ou quando o remetente não corresponde ao registo.

Países que adotaram esta medida: Espanha, Finlândia, França, Irlanda, Itália, Polónia e Reino Unido.

3. **Registo de números proibidos "Do-not-originate" (DNO)**

É criada uma base de dados nacional de números que nunca podem ser usados para identificadores de chamadas de saída, também conhecida como uma lista *"Do-not-Originate*" (DNO), a não ser pelos sistemas autorizados para tal.

Nesta lista são geralmente incluídos números de telefone de serviços de emergência, serviços bancários e outros serviços públicos ou privados cuja impersonificação por ciber-criminosos pode trazer danos para o País.

Países que adotaram esta medida: Alemanha, Bélgica, Irlanda, Polónia, Reino Unido e República Checa.

4. **Registo de números não atribuídos**

É mantida, pelo Regulador das Telecomunicações, uma lista de números que não foram atribuídos e que não podem ser usados para originar chamadas – por exemplo, CLI vazio, não atribuído a nenhum serviço ou que não esteja conforme o plano nacional de numeração - devendo os operadores bloquear proactivamente as comunicações com origem nestes números.

Países que adotaram esta medida: Espanha, Irlanda, República Checa