MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

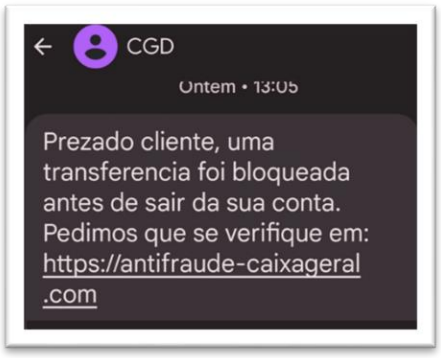
12 de março de 2024

'*Phishing*' dirigido a clientes da Caixa Geral de Depósitos

1. Está em curso uma campanha de ***phishing*** que tem em vista aceder, de forma ilícita, a contas bancárias de clientes da ***Caixa Geral de Depósitos***, para delas retirar montantes monetários. Não se trata, como também tem ocorrido frequentemente noutros casos, de uma mera campanha criminosa para obtenção de dados de cartões bancários de pagamento de clientes da *Caixa Geral de Depósitos*. Esta nova campanha é uma iniciativa de **engenharia social mais agressiva**, que pretende gerar imediatos e elevados lucros ilícitos aos agentes criminais, com prejuízo das vítimas.

2. Como na generalidade dos casos de *phishing*, este procedimento criminoso passa pela expedição, pelos agentes do crime, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas. Em casos anteriores foi muito utilizado o correio eletrónico ou o serviço de mensagens *WhatsApp*. Na presente campanha, além de **mensagens *WhatsApp***, foi também identificado o regular uso de **mensagens de SMS**.
Esta campanha, já identificada no início de 2024, intensificou-se nas últimas semanas.

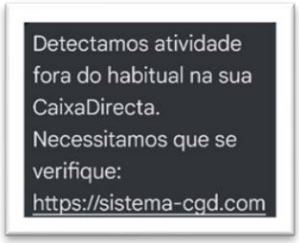
3. Como costuma ocorrer com outras campanhas de *phishing*, o teor das mensagens fraudulentas tem evoluído e variado ao longo das semanas, consoante o grupo criminoso que leva a cabo a campanha. Porém, todas as mensagens referem sempre terem como origem "*CGD*", com isso pretendendo convencer os destinatários de que foram emitidas pela *Caixa Geral de Depósitos*.



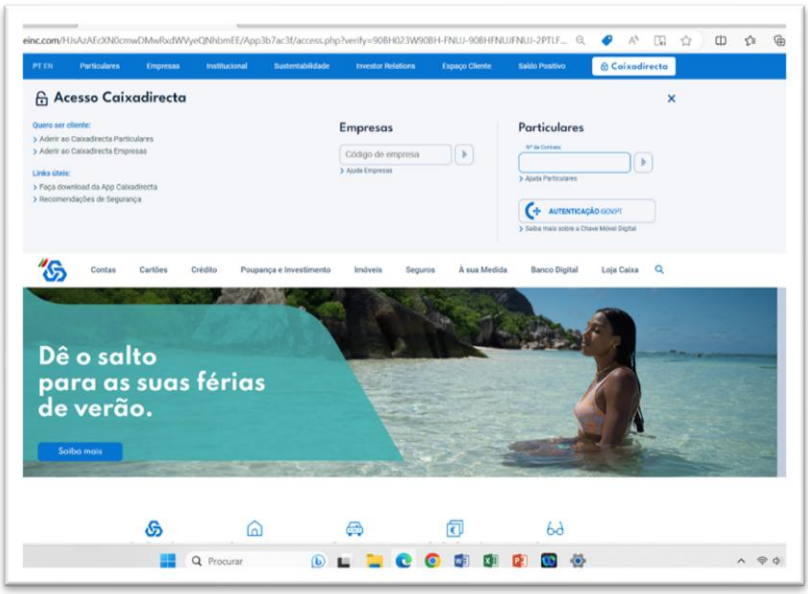
Além disso, estas mensagens pretendem sempre dar a entender que correspondem a um procedimento de segurança, alertando o respetivo destinatário para um "movimento", ou um "acesso", ou outro "incidente anormal" na respetiva conta bancária.

4. Por último, todas estas mensagens incitam ao acesso urgente a essa conta, para "verificação", ou "confirmação", ou para "evitar bloqueio". Para o efeito, todas elas indicam um *link*, que permitirá ao destinatário o acesso direto à sua conta bancária. Os diversos *links* identificados incluem invariavelmente

alguma palavra, ou pelo menos algumas letras, que correspondem ao nome ou à sigla ou abreviatura da *Caixa Geral de Depósitos*, de forma a dar-lhes verosimilhança.
Porém, não correspondem ao autêntico URL utilizado pela página *web* da *Caixa Geral de Depósitos*.

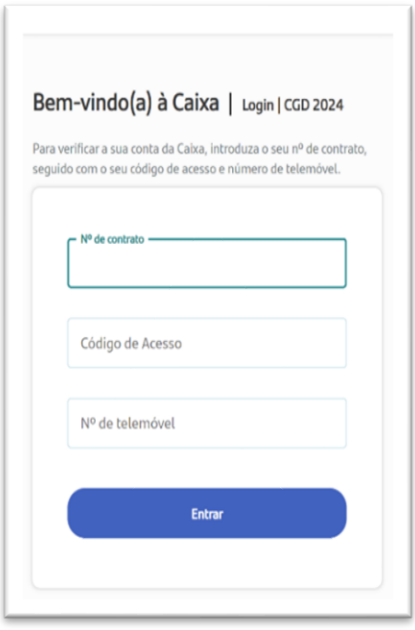


5. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes da *Caixa Geral de Depósitos*: não são remetidas pela *Caixa Geral de Depósitos* nem a partir de sistemas informáticos pertencentes a esta entidade.



6. Do mesmo modo, os *links* incluídos nas mensagens fraudulentas, não conduzem ao verdadeiro *site* da *Caixa Geral de Depósitos*: se acedidos, encaminham para uma página *web* que exibe imagens e logotipos normalmente por ela utilizados, mas que não correspondem à verdadeira página da *Caixa Geral de Depósitos*. Tais *sites* correspondem a variados e diferentes URL, que se vão multiplicando e desaparecendo poucos dias depois (consoante os fornecedores de serviço Internet onde estão alojados vão detetando o respetivo teor fraudulento e, consecutivamente os vão desativando).

7. Foram identificados nesta campanha *sites* fraudulentos especificamente desenhados para computadores, mas também outros especificamente construídos para *browsers* de dispositivos móveis – isto é, *sites* especificamente desenhados para serem abertos em telemóveis com acesso à Internet. Neste último caso, foram ainda identificadas situações em que o *link* fornecido pelos agentes criminosos abre uma página *web* que simula o aspeto gráfico da aplicação (*App*) para telemóveis da *Caixa Geral de Depósitos.*



8. Em todos os casos identificados, quando a vítima acedeu ao *link* que lhe foi remetido pela mensagem fraudulenta, além de aceder a uma suposta página da *Caixa Geral de Depósitos*, ainda lhe foi pedido que introduzisse as suas credenciais de acesso à sua conta bancária (designadamente, o seu número de contrato e o seu código de acesso).

Invariavelmente, foi-lhe também pedido que introduzisse o seu número de telemóvel.

Após esta última solicitação, a vítima foi sempre informada de que deveria aguardar um contacto telefónico da *Caixa Geral de Depósitos*, o que deveria acontecer muito brevemente – na generalidade dos casos, foi referido à vítima que tal contacto ocorreria nas seguintes 24 horas.

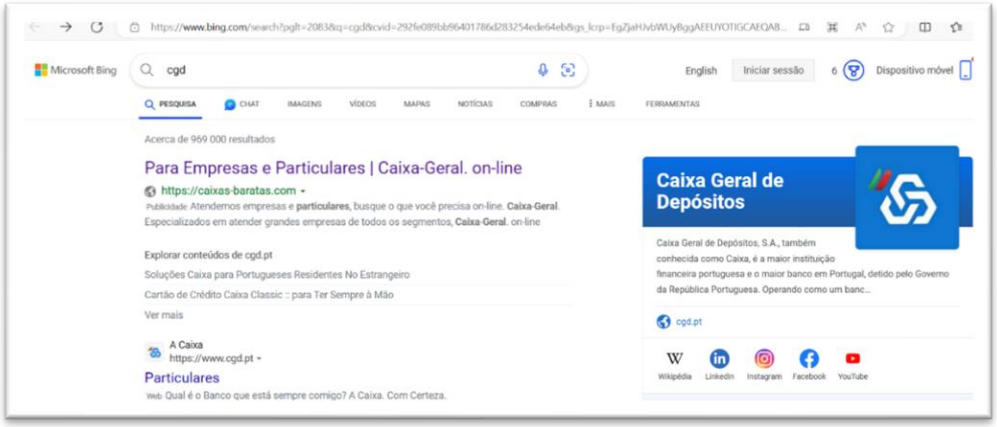
9. Porém, nenhum destes *sites*, que solicitam estas informações às vítimas, é gerido pela *Caixa Geral de Depósitos* nem é por ela autorizado. Embora o endereço URL (*link*) fornecido seja muito vagamente semelhante, ou aluda a partes do nome da verdadeira página daquele banco na Internet, todos estes *sites* são *páginas falsas* que, fraudulentamente, pretendem simular ser a autêntica página *web* daquela entidade bancária.

10. Foram identificadas nas últimas semanas diversas páginas fraudulentas associadas a esta campanha criminosa, em geral relacionadas com prestadores de serviço de alojamento e partilha gratuita de domínios DNS na *cloud*.

Todas elas pretendem imitar a aparência, aos olhos do utilizador comum, da autêntica página da *Caixa Geral de Depósitos* ou da aplicação (*App*), para telemóvel, da *Caixa Geral de Depósitos*. Por este processo criminoso, os seus autores pretendem induzir as vítimas a facultarem-lhes as suas credenciais de acesso às suas contas bancárias e os seus números de telemóvel.

11. Têm também ocorrido casos em que o método utilizado pelos agentes criminosos para atrair o acesso de vítimas a páginas *falsas* não é o das mensagens fraudulentas. Foram identificados casos em que as vítimas foram induzidas a visitar tais páginas após pesquisas em motores de busca, por anúncios fraudulentos.

Isto é, na altura em que quiseram aceder ao *site* da *Caixa Geral de Depósitos*, as vítimas optaram por procurar o concreto *link* do mesmo em motores de pesquisa (Google, Bing…). Como resultado, encontraram anúncios fraudulentos que, sem que as vítimas se aperceberem, as encaminharam para as páginas *falsas*.



12. O restante processo ilícito passa pela utilização, pelos agentes criminosos, das credenciais de acesso à conta bancária e do número de telemóvel da vítima.
O propósito dos agentes criminosos é transferir quantias daquela conta para uma outra, por eles controlada. Para o efeito, usam as credencias bancárias da vítima para aceder à conta desta. Porém, como sabem que a transferência de quantias monetárias a partir de contas da *Caixa Geral de Depósitos* exige um segundo fator de autenticação (designadamente um código emitido por SMS para o telefone do respetivo titular), abordam telefonicamente a vítima, procurando induzi-la em erro, com o objetivo de obter esse código.

13. Assim, munidos das credenciais, os agentes criminosos acedem à conta da vítima e verificam as quantias que nela possam estão depositadas. Depois, ligam para o número de telemóvel da vítima. Dizem-lhe serem agentes da área da segurança informática da *Caixa Geral de Depósitos* e mostram conhecer os detalhes da conta e os últimos movimentos da mesma – o que conseguem por terem tido acesso a tal conta, com as credenciais facultadas pela própria vítima.
Desenvolvem o processo fraudulento dizendo à vítima que foi detetada uma avultada transferência bancária suspeita, a partir daquela conta. Por isso, pedem à vítima que confirme a autenticidade dessa transferência, que sabem não ter existido. Perante esta informação, a vítima nega que tenha sido ela a autora de tal transferência e pede que a mesma seja cancelada. Porém, os agentes criminosos informam que não podem cancelar tal transferência apenas por conversação telefónica, tendo a vítima que facultar-lhes um código de autenticação que a mesma há-de receber por SMS.

14. Em simultâneo, tendo acesso à conta da vítima, sem que a mesma disso se aperceba, os agentes criminosos geram uma ordem de transferência bancária para uma outra conta, por eles gerida. Sabem que este tipo de ordem dá automaticamente origem à emissão de um código de autenticação, que é remetido para o telemóvel do titular da conta bancária.
Por isso, de seguida e pelo telefone, perguntam à vítima se recebeu um código, informando-a de que tal código será o tal que é necessário para cancelar a transferência fraudulenta – quando na verdade se trata do código requerido pelo sistema informático da *Caixa Geral de Depósitos* para validar a transferência que eles efetiva e fraudulentamente ordenaram.

Muitas vítimas têm facultado tal código aos agentes criminosos, julgando estarem a falar com o funcionário bancário. Deste modo, habilitam os agentes criminosos a concretizar a transferência que planearam. E a vítima é defraudada no respetivo montante.

15. Embora a campanha em curso vise especificamente clientes da *Caixa Geral de Depósitos*, foram já identificadas outras, visando clientes de outras instituições bancárias.

16. Mensagens de SMS ou *WhatsApp* como as que acima se descreveram, incitando ao acesso a páginas de bancos *online*, devem ser ignoradas e apagadas, sem resposta.
Telefonemas como os que se referiram, que supostamente têm origem em departamentos de segurança de bancos, devem ser cuidadosamente avaliados. A respetiva autenticidade deve ser confirmada com o gestor de cliente, ou outro funcionário ou representante bancário.
Caso a vítima, sem se aperceber, acabe por facultar aos agentes criminosos os dados de acesso à sua conta bancária, importará, como primeira diligência a empreender, alterar as respetivas credenciais de acesso e contactar o banco em causa.