MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

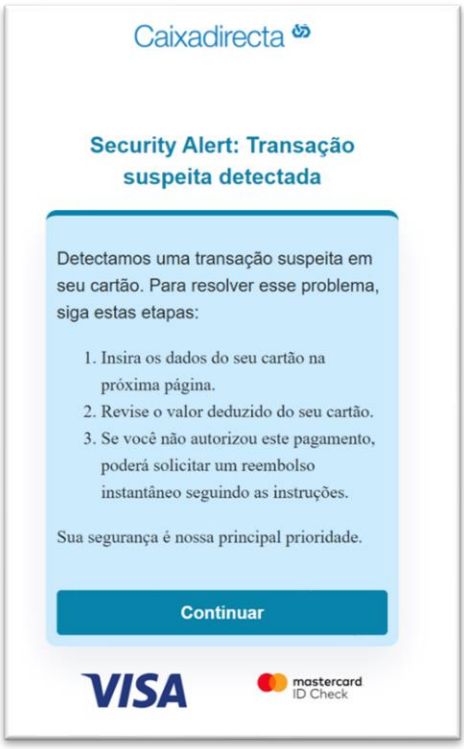
16 de novembro de 2023

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

1. Está em curso mais uma campanha de *phishing* que tem em vista obter, de forma ilícita, os dados dos cartões bancários de vítimas indiscriminadas. Esta campanha dá continuidade a várias outras, que ocorreram no passado. No caso presente, os agentes criminosos procuram, com a campanha, atingir clientes da *Caixa Geral de Depósitos* que sejam titulares de cartões bancários de pagamento.

2. Como em todos os casos de *phishing*, o processo criminoso começou com a expedição, para muitíssimos destinatários, de mensagens fraudulentas – noutros casos foi utilizado o correio eletrónico ou o serviço de mensagens *WhatsApp*. Na presente campanha foi identificado o uso de mensagens de SMS. A primeira das mensagens desta campanha sinalizada pelo Gabinete Cibercrime foi referenciada a 15 de novembro de 2023, às 9 horas e 30 minutos.

3. Destas mensagens consta o seguinte texto: "*Seu pagamento com cartão foi realizado com sucesso! Se você suspeita que esta transacao nao e autorizada, cancele-a clicando aqui*", indicando de seguida um *link*. Este *link* supostamente facilita o acesso à conta bancária do destinatário. A mensagem inclui a indicação, como remetente, das iniciais "*C.G.D.*".



Como habitual, noutras campanhas criminosas desta natureza, incita-se o destinatário a ação imediata - designadamente, a aceder ao *link* facultado, para "*cancelar a transação*".

4. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes da *Caixa Geral de Depósitos*. Não foram remetidas pela *Caixa Geral de Depósitos* nem a partir de sistemas informáticos pertencentes à mesma.

Por sua vez, o *link* incluído nas mensagens fraudulentas conduz a um *site* Internet com um URL diferente daquele que aparenta, embora encaminhe para uma página *web* que exibe imagens e logotipos normalmente utilizados pela *Caixa Geral de Depósitos*.

5. Tal página informa imediatamente, sem que o "cliente" tenha que identificar-se ou facultar qualquer credencial de acesso, que

o respetivo cartão foi objeto de uma "*transação suspeita*", sendo-lhe dadas instruções "*para resolver esse problema*".

6. Logo de seguida, abre-se uma nova página em que é solicitado à vítima que introduza os dados do seu cartão bancário – o número do mesmo, a data de validade e o código CVV (*Card Verification Value*). Isto é, na prática, é pedido à vítima que faculte os dados que permitem utilizar o cartão em causa.

7. Porém, este *site*, onde estas informações são introduzidas, não é gerido pela *Caixa Geral de Depósitos* nem por ela autorizado. Embora o endereço URL seja vagamente semelhante ao da verdadeira página daquele banco na Internet, esta trata-se de uma página falsa, que pretende simular ser a autêntica página *web* daquela entidade bancária.
A página fraudulenta está registada no *registrar* "*Easyname GmbH*" (http://www.easyname.com), com sede em Salzburgo, na Áustria mas, na verdade os seus servidores de DNS apontam para a plataforma "*FreeDNS*" (https://freedns.afraid.org/), prestador de serviço de alojamento e partilha gratuita de domínios DNS na *cloud* (com sede física em Granite Bay, na Califórnia, Estados Unidos da América).

8. Esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da *Caixa Geral de Depósitos*. Por este processo criminoso, os seus autores pretendem induzir a vítima a facultar-lhes dados dos seus cartões. Se a vítima introduzir a informação que se lhe solicita (os dados do cartão bancário), estará a facultar aos agentes criminosos informação que lhes permite utilizarem abusivamente os dados daquele cartão, em seu prejuízo.

9. Mensagens como as que acima se descreveram devem ser ignoradas e apagadas, sem resposta. Caso a vítima se aperceba de que acabou por facultar aos agentes criminosos os dados do seu cartão, importará, como primeira diligência a empreender, contactar o banco emissor e proceder ao cancelamento daquele cartão.