ALERTA CIBERCRIME

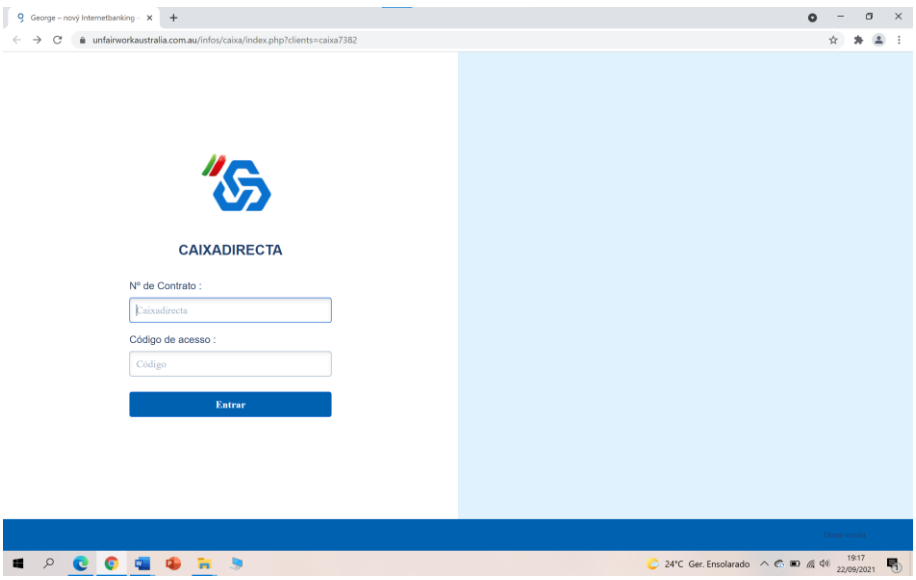
27 de setembro de 2021

'Phishing' dirigido a clientes da Caixa Geral de Depósitose e titulares de cartões de crédito

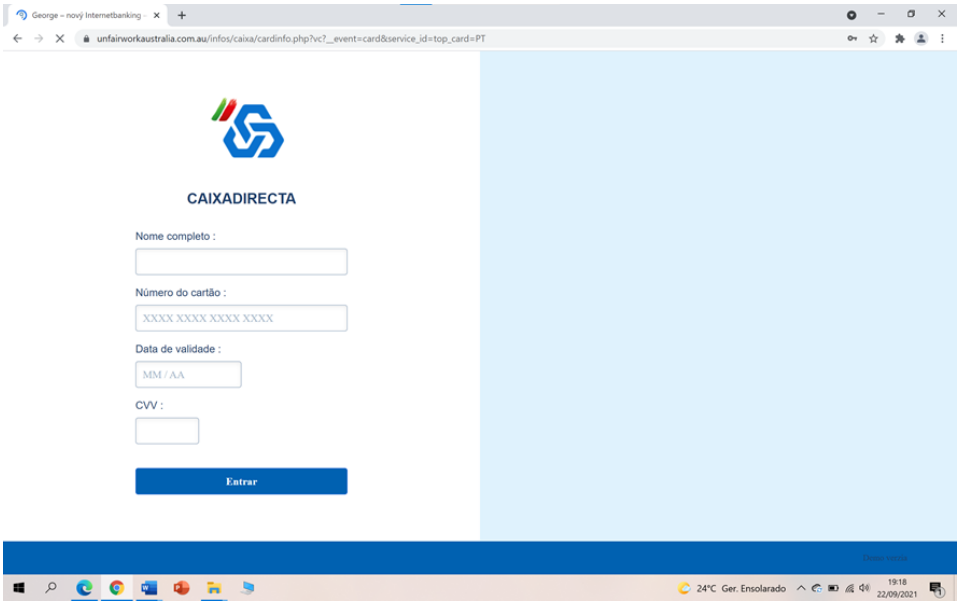
1. Está em curso uma campanha de *phishing*, dirigida a vítimas que sejam simultaneamente clientes da Caixa Geral de Depósitos e titulares de cartões de crédito. Nesta campanha, os seus autores pretendem convencer as vítimas a facultarem-lhes dados dos seus cartões de crédito.

2. Como habitual em casos de *phishing*, o processo criminoso começa com a expedição, para muitos destinatários, de mensagens fraudulentas – no caso desta campanha, foram identificadas mensagens de SMS, a partir de 22 de setembro. Nestas mensagens diz-se que a "*Sua conta online está temporariamente suspensa devido a atividades suspeitas. Faça login e verifique suas informações*". De seguida indica-se um *link*, o qual o destinatário deverá aceder.
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 ou números telefónicos pertencentes a esta instituição bancária.

3. O *link* que se referiu, contido nas mensagens fraudulentas, conduz a um *site* Internet que, embora grosseiramente, pretende aparentar ser o da Caixa Geral de Depósitos, exibindo o logotipo corporativo utilizado por aquela.



Inclui espaços em que se solicita a introdução de dados respeitantes à conta bancária da vítima: o número do respetivo contrato e o código de acesso. Caso o utilizador introduza estes dados, de acesso à sua conta bancária, abre-se uma nova página *web* em que lhe é solicitado que introduza os dados respeitantes ao seu cartão de crédito: o nome completo ali gravado, o número do cartão, a respetiva data de validade e ainda o código de segurança (CVV).

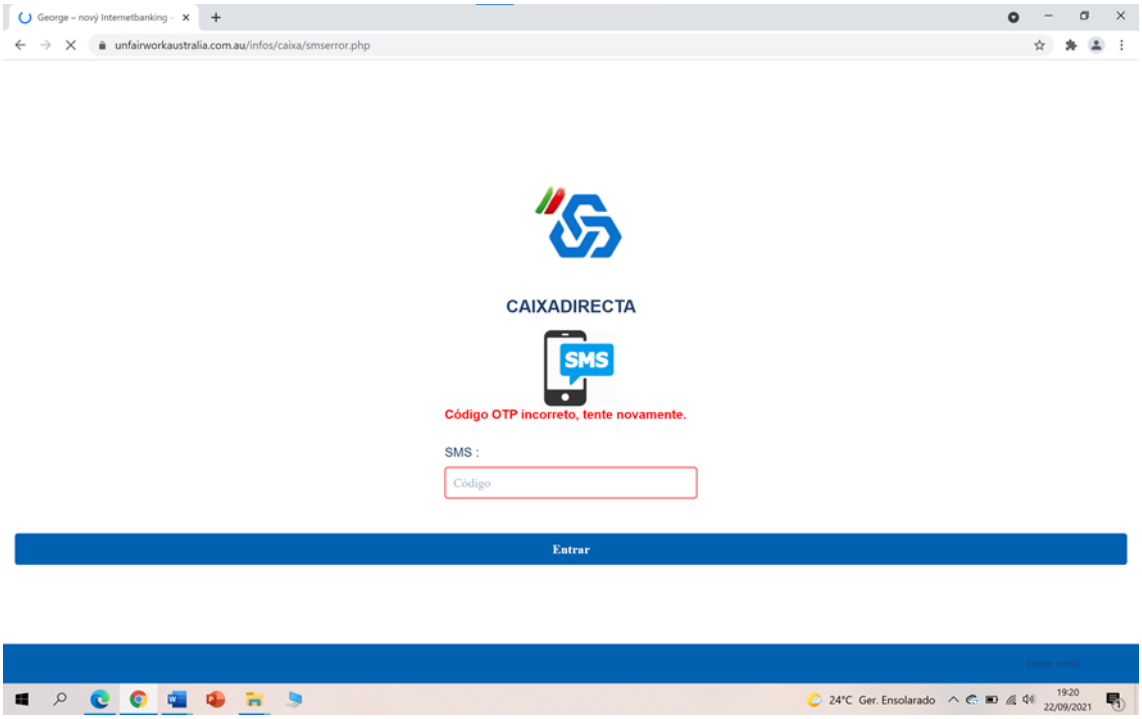


4. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da Caixa Geral de Depósitos. Se a vítima nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos, além do mais, todos os dados do seu cartão de crédito, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

5. Aliás, imediatamente após o utilizador inserir os dados do seu cartão de crédito naquela página, os agentes criminosos usam os mesmos, efetuando de imediato compras *online*.
Como o procedimento de compras *online* requere, com frequência, confirmação das mesmas mediante a introdução de um código (*token*) expedido por mensagem escrita (SMS) para o telefone do titular do cartão, este método criminoso prevê essa possibilidade. Assim, depois da introdução dos dados do cartão de crédito na página falsa, abre-se uma nova página, supostamente do servidor da Caixa Geral de Depósitos.

Nesta nova página o utilizador é informado de que "*Você receberá um código SMS OTP para confirmar o número de telefone*", sendo deixado espaço para se inserir tal código.

6. Efetivamente, logo que o criminoso efetua a primeira compra, a vítima (que é a legítima titular do cartão de crédito utilizado) recebe um código, por SMS, no seu telefone. Se o introduzir na página falsa permite ao criminoso autenticar e efetivar aquela compra.
Porém, recorrentemente, na página surge uma mensagem de erro: "*Código OTP incorreto, tente novamente*". O propósito deste procedimento é permitir ao criminoso efetuar uma segunda compra, e uma outra, e ainda outras, até que a vítima, por estranhar ou outra razão, deixe de inserir os códigos na página.



7. Este *site* não é gerido pela Caixa Geral de Depósitos nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página daquela instituição bancária. O nome de domínio desta página fraudulenta está registado no fornecedor de serviços "*Webcentral*" (https://www.webcentral.com.au), um *registrar* com sede em Melbourne, na Austrália, especializado no fornecimento de nomes de domínio e outros serviços de Internet. Pertence à sociedade *Roselands Computer Company Ltd*, com sede em Sydney, igualmente na Austrália.

8. Como se disse, este método criminoso tem como objetivo e único propósito capturar os dados dos cartões de crédito das vítimas, para serem usados indevida e abusivamente. Mensagens como as acima descritas devem ser apagadas. Caso o utilizador introduza os dados na página a que se acede pelo *link* facultado pelos agentes do crime, importará, como primeira diligência a empreender, proceder ao cancelamento do cartão.