# ALERTA CIBERCRIME

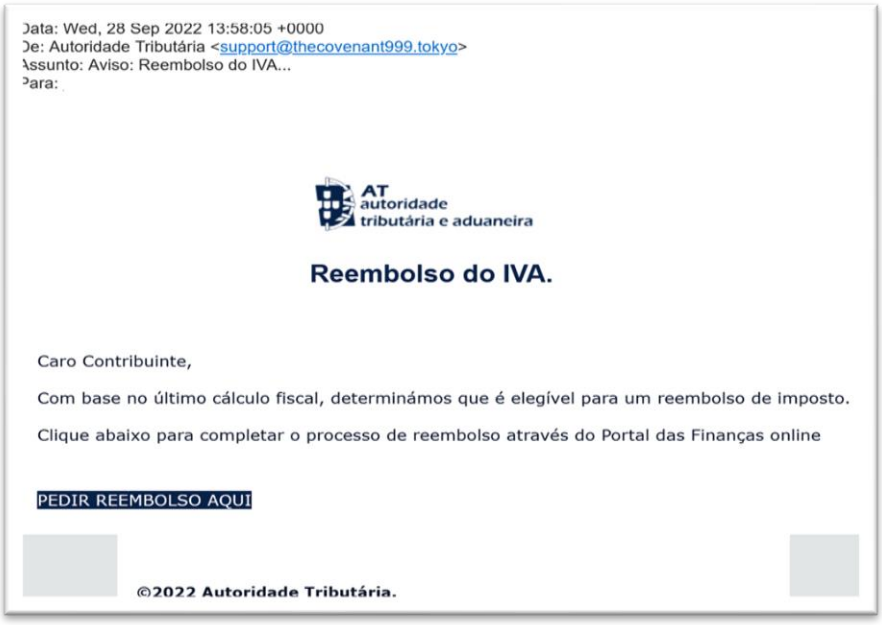
**29 de setembro de 2022**

## *'Phishing'* de cartões bancários usando a imagem da Autoridade Tributária

**1.** Está em curso uma campanha criminosa de *phishing*, usando abusivamente a imagem da Autoridade Tributária, dirigida a vítimas que sejam titulares de cartões bancários de débito ou de crédito. Nesta campanha, os seus autores pretendem convencer as vítimas a facultar-lhes todos os dados dos seus cartões bancários, com o argumento de que pretendem reembolsar-lhes quantias respeitantes a pagamento excessivo de impostos (supostamente IVA).

**2.** Como habitual em casos de *phishing*, o processo começa com a expedição, para muitos destinatários, de forma indiscriminada e aleatória, de mensagens fraudulentas de correio eletrónico. Registaram-se campanhas anteriores idênticas durante o ano de 2020, durante o ano de 2021 e também já em 2022. Agora, foram sinalizadas pelo Gabinete Cibercrime concretas mensagens desta campanha, com mais intensidade, a partir da tarde de 28 de setembro de 2021.

**3.** Nestas mensagens, com o título no assunto, "*Aviso: Reembolso do IVA*", dirigindo-se as mesmas a "*Caro Contribuinte*", anuncia-se que "*Com base no último cálculo fiscal, determinámos que é elegível para um reembolso de imposto*". Despois, incita-se o mesmo: "*Clique abaixo para completar o processo de reembolso através do Portal das Finanças online*", indicando-se de forma muito destacada um botão com a legenda "PEDIR REEMBOLSO AQUI". As mensagens vêm assinadas com a expressão *"©2022 Autoridade Tributária*" e incluem um logotipo normalmente utilizado por aquela entidade pública.


Data: Wed, 28 Sep 2022 13:58:05 +0000
De: Autoridade Tributária <support@thecovenant999.tokyo>
Assunto: Aviso: Reembolso do IVA...
Para:

AT autoridade tributária e aduaneira

Reembolso do IVA.

Caro Contribuinte,

Com base no último cálculo fiscal, determinámos que é elegível para um reembolso de imposto.

Clique abaixo para completar o processo de reembolso através do Portal das Finanças online

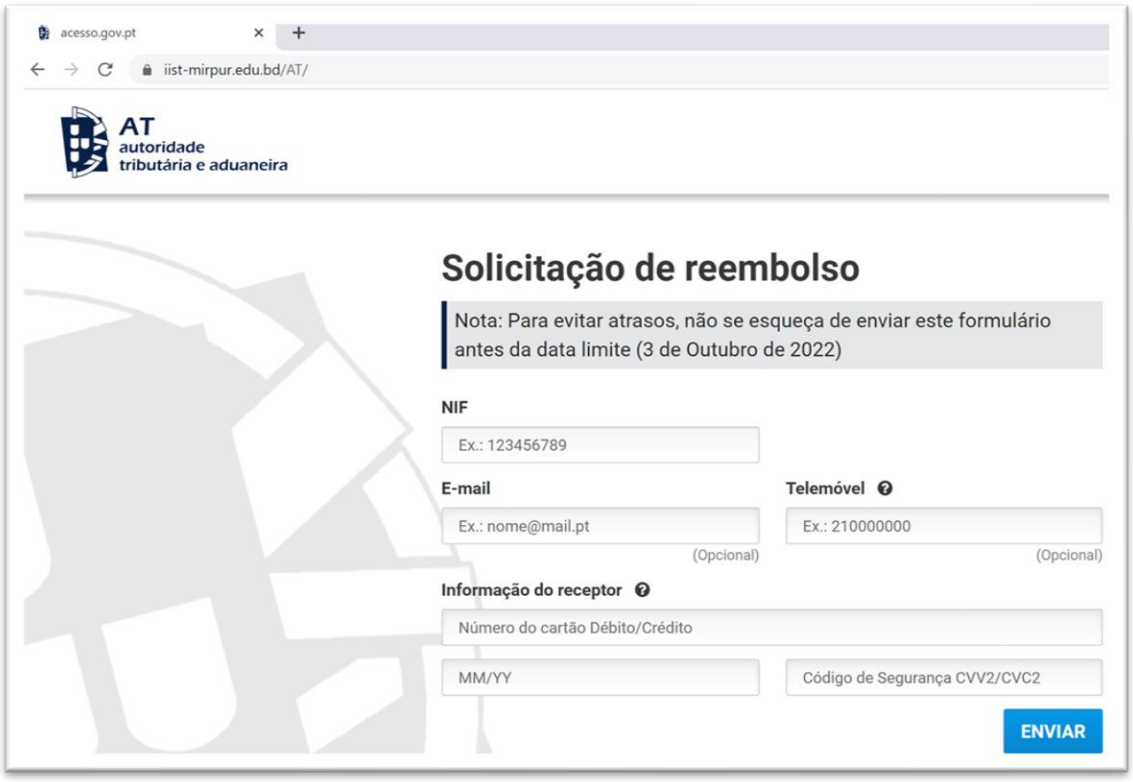
PEDIR REEMBOLSO AQUI

©2022 Autoridade Tributária.

**4.** Trata-se de mensagens fraudulentas, não provenientes da Autoridade Tributária: não foram remetidas pela Autoridade Tributária nem a partir de sistemas informáticos pertencentes a esta entidade pública.

**5.** Aparentemente, tais mensagens foram remetidas da caixa de correio "*Autoridade Tributária*", mas na verdade não é assim. Provieram de endereços de diversos servidores, ou de contas de correio eletrónico ilegitimamente acedidas pelos criminosos e abusivamente usadas para este específico efeito. Nalguns dos casos identificados, esse endereço foi *mascarado*, para que a informação que fica visível ao destinatário o levasse a concluir que provinha de info@portaldasfinancas.gov.pt.

**6.** Por sua vez, o *link* que se referiu, assinalado com a expressão "PEDIR REEMBOLSO AQUI", contido nas mensagens fraudulentas, conduz a um s*ite* na Internet que aparenta ser o da Autoridade Tributária, exibindo uma imagem gráfica e um logotipo normalmente utilizados por aquela autoridade pública. Nessa página, solicita-se ao utilizador que introduza os seus dados pessoais e, entre eles, o número do seu cartão bancário, a respetiva data de validade e ainda o código de segurança (CVV) do mesmo.

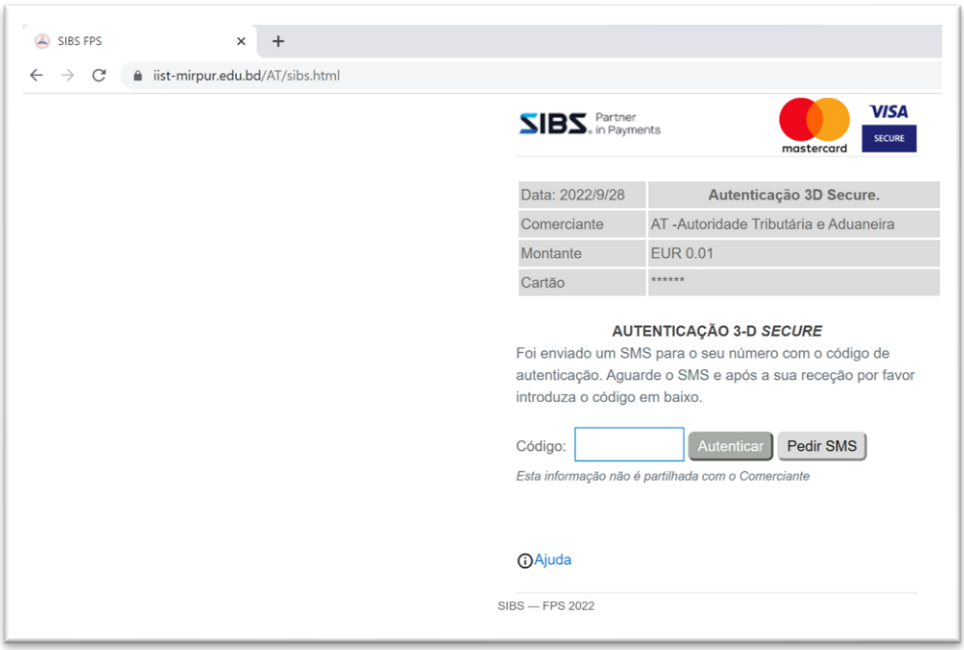



**7.** Este *site* não é gerido pela Autoridade Tributária nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página da Autoridade Tributária. Tem como único propósito captar os dados de cartão bancário das vítimas – os quais serão depois abusivamente utilizados pelo agente do crime.

No decurso desta campanha, como tem acontecido recorrentemente com outras campanhas de *phishing*, os criminosos têm feito alojar esta página falsa em sucessivos servidores de alojamento na *cloud*, os quais permitem a contratação *online*, sem que possa apurar-se a identidade do seu dono.

**8.** Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da Autoridade Tributária. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados do seu cartão bancário, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

**9.** Aliás, em geral, 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, nalguns casos, 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 SIBS (*SIBS - Forward Payment Solutions, SA*., anteriormente denominada *SIBS - Sociedade Interbancária de Serviços, SA*), em que solicitado que se autentique o pagamento com o código recebido por telefone.




**10.** Efetivamente, logo que o criminoso efetuar a compra *online*, a vítima recebe um código, por SMS. Se o introduzir na página falsa permite ao criminoso autenticar e efetivar aquela compra.

**11.** Como se disse, este método criminoso tem como objetivo obter dados de cartões de crédito das vítimas, para que os criminosos os possam usar indevidamente. Mensagens como as acima descritas devem ser ignoradas, sem se aceder ao *link* facultado e sem se inserir a informação dos cartões solicitada. Caso tal aconteça, importará, como primeira diligência a empreender, proceder ao cancelamento daqueles cartões.