



ALERTA CIBERCRIME

8 de outubro de 2026

'Phishing' – Banco CTT

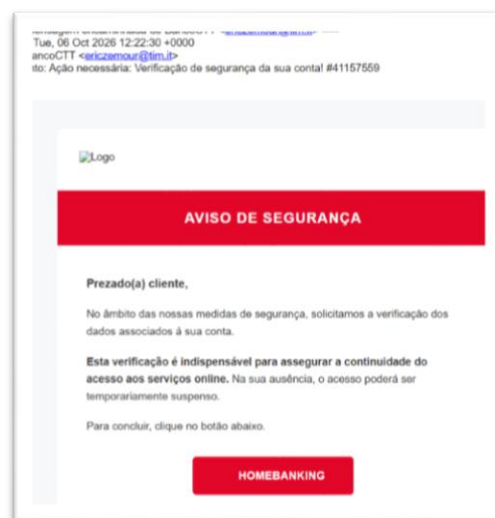
1. Estão em curso campanhas criminosas múltiplas pelas quais, por meio de técnicas de **phishing**, os agentes criminosos procuram obter de forma ilícita os códigos de acesso a contas de clientes do *Banco CTT*, para depois fazerem uso das mesmas em seu proveito económico, transferindo valores para contas por si controladas. Trata-se de campanhas de *phishing* bancário, que podem provocar avultados prejuízos patrimoniais aos clientes daquele banco.

2. Como na generalidade dos casos de *phishing*, este método criminoso começa com a expedição, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas – no caso destas campanhas criminosas, mensagens de correio eletrónico. A diversidade de mensagens identificada nas semanas recentes permite concluir que as campanhas estão a ser desenvolvidas por diferentes grupos, que competem entre eles nestes propósitos criminosos.

3. Em todas estas mensagens se menciona que o remetente é o *Banco CTT*, nelas se incluindo o respetivo logotipo e procurando reproduzir-se a correspondente gráfica corporativa. Os textos das mensagens também pretendem convencer os destinatários de que foi aquela instituição bancária quem as emitiu.

Foram identificadas variantes destas campanhas mas, em geral, todas as mensagens apelam aos destinatários para que acedam à página do *Banco CTT* na Internet para a "*atualização imediata de dados*". São invocadas "*razões de segurança*" e é insistentemente sublinhada a necessidade emergente desta ação do destinatário, sob pena de bloqueio do acesso à conta bancária. É indicado nas mensagens um *link* para o efeito.

4. O teor destas mensagens é enganoso e fraudulento, pretendendo fazer crer os respetivos destinatários de que tais mensagens têm origem no *Banco CTT* e, com isso, incutir neles a convicção de que as mensagens são legítimas e autênticas. Porém, isso não corresponde à verdade: estas mensagens não foram remetidas pelo *Banco CTT* nem a partir de servidores daquela entidade bancária ou por ela geridos.





O apelo à urgência na reação tem em vista induzir uma ação menos refletida e ponderada das potenciais vítimas.

5. Todas as mensagens incluem um *link* (por vezes, embutido num botão gráfico) que, se acedido, leva a vítima a uma página fraudulenta, que pretende imitar a página *oficial* do *Banco CTT* e a respetiva imagem gráfica corporativa, mas que não corresponde à autêntica página *web* daquela entidade.

6. Nesta página, é solicitado à vítima que insira os seus códigos pessoais de acesso à conta do *Banco CTT*. Caso a vítima insira os seus dados de acesso naquela página fraudulenta, está a facultar aos agentes criminosos a informação que permite aos mesmos aceder à sua conta.

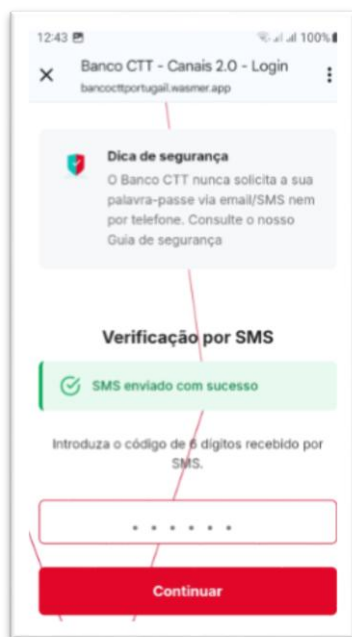
7. Foram identificadas variantes destas campanhas em que, na página que fraudulentamente imita a página do *Banco CTT*, além dos dados de acesso à conta bancária, são também solicitados os dados do cartão bancário da vítima: o nome ali gravado, o número do cartão, a respetiva data de validade e ainda o código de segurança (CVV).

Esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página do *Banco CTT*. Se a vítima introduzir nela a informação que se lhe solicita, fornecerá aos agentes criminosos, além do mais, todos os dados do seu cartão de crédito, permitindo assim àqueles que venham a utilizar este cartão, em compras ou pagamento de serviços.



8. Nas variantes de obtenção de dados de cartões bancários, imediatamente após o utilizador inserir os dados do seu cartão na página fraudulenta, os agentes criminosos usam os mesmos, efetuando de imediato compras *online*. Como o procedimento de compras *online* requiere 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: depois da introdução dos dados do cartão de crédito na página falsa, abre-se um novo menu em que é solicitado um código de autenticação. Logo que o agente criminoso efetuar uma compra *online*, a vítima recebe esse por SMS, no seu telefone. Se o introduzir na página falsa, como lhe é pedido, permite ao criminoso autenticar e efetivar aquela compra.

9. Têm sido identificadas páginas falsas do *Banco CTT* em diversos servidores (alojadas em também diversos prestadores de serviços na *cloud*). Nenhuma delas é, naturalmente, por aquele banco autorizada. São páginas não





MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

verdadeiras, que pretendem imitar a autêntica página daquela instituição bancária.

10. O propósito dos agentes criminosos é o de, utilizando os dados de acesso às contas bancárias das vítimas, vir com isso a beneficiar economicamente. Na variante de captura de dados de cartões bancários das vítimas, o propósito dos criminosos é o de vir a utilizá-los indevida e abusivamente, em compras *online*.

Mensagens de correio eletrónico como as que acima se descreveram devem ser ignoradas e apagadas, sem resposta.

Caso a vítima acabe por facultar aos agentes criminosos os dados de acesso à sua conta bancária ou os dados do seu cartão bancário, importará, como primeira diligência a empreender, contactar o banco (ou o emissor do cartão) pelas formas e canais habituais.