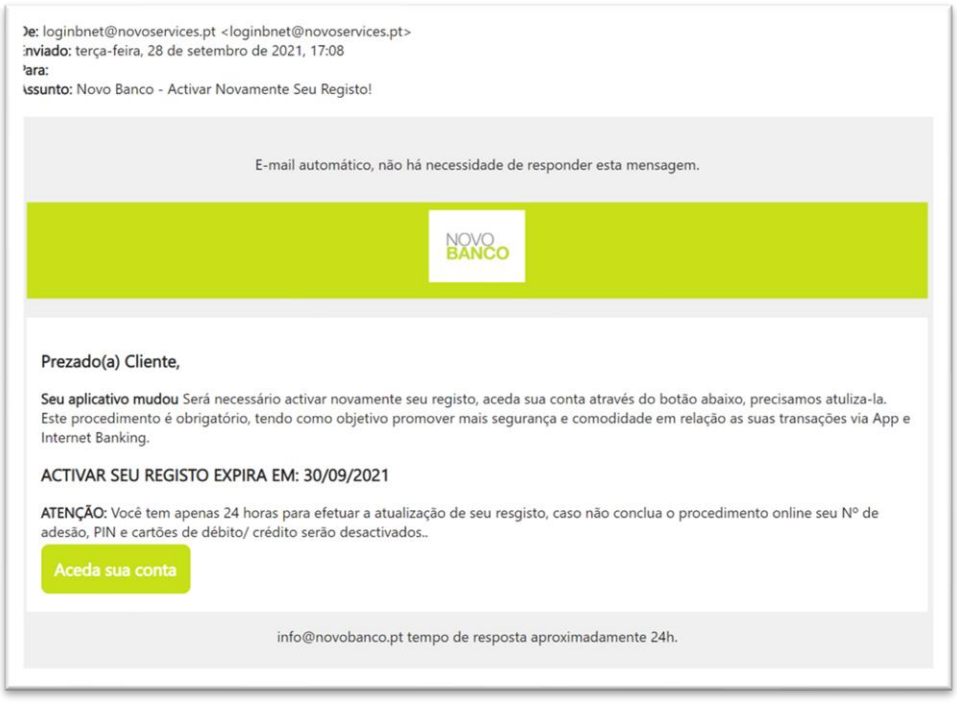
ALERTA CIBERCRIME

29 de setembro de 2021

'*Phishing*' dirigido a clientes do Novobanco

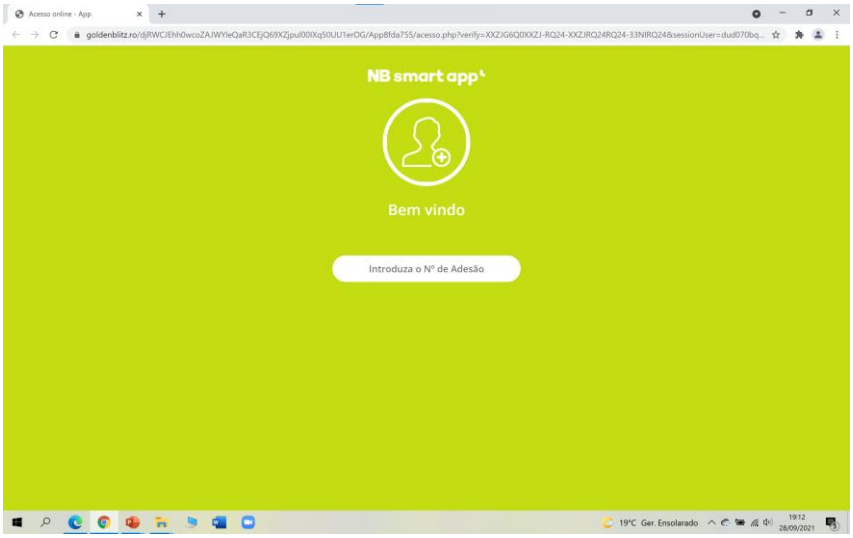
1. Está em curso uma campanha de "*phishing*", dirigida a clientes do *Novobanco*. Como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira das mensagens desta campanha sinalizada pelo Gabinete Cibercrime foi referenciada a 28 de setembro de 2021, às 17 horas e 28 minutos.

2. Nestas mensagens, com título, no assunto, "*Novo Banco - Activar Novamente Seu Registo*!" refere-se que o "aplicativo" daquele banco "*mudou e será necessário ativar novamente seu registo, aceda sua conta através do botão abaixo, precisamos atualizá-la. Este procedimento é obrigatório, tendo como objetivo promover mais segurança e comodidade em relação as suas transações via App e Internet Banking*". Ainda se adianta que "*ACTIVAR SEU REGISTO EXPIRA EM: 30/09/2021" e que "ATENÇÃO: Você tem apenas 24 horas para efetuar a atualização de seu registo, caso não conclua o procedimento online seu Nº de adesão, PIN e cartões de débito/ crédito serão desativados*.".

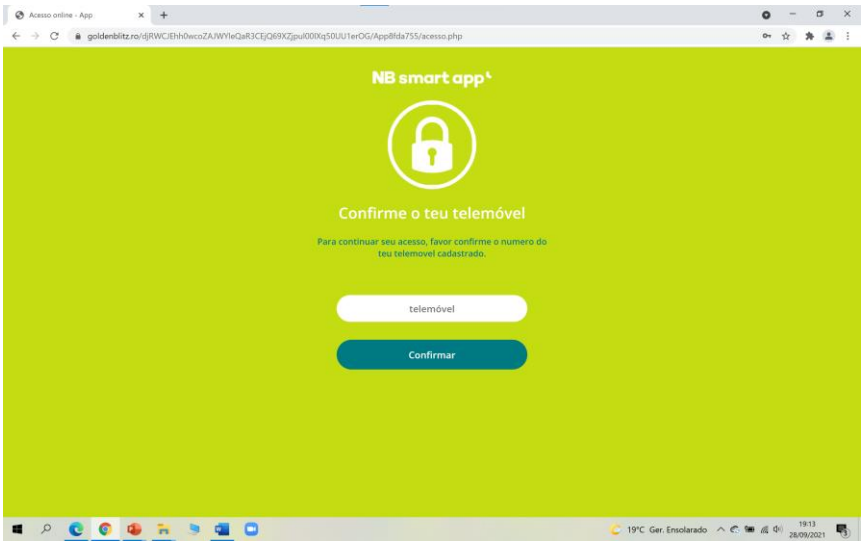


3. Ainda se inclui um botão com um *link*, supostamente para facilitar o acesso à conta bancária do destinatário. Incluiu-se, por último, uma assinatura, com a indicação do endereço info@novobanco.pt.
Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do *Novo Banco*. Não foram remetidas pelo *Novo Banco* nem a partir de sistemas informáticos pertencentes ao mesmo.

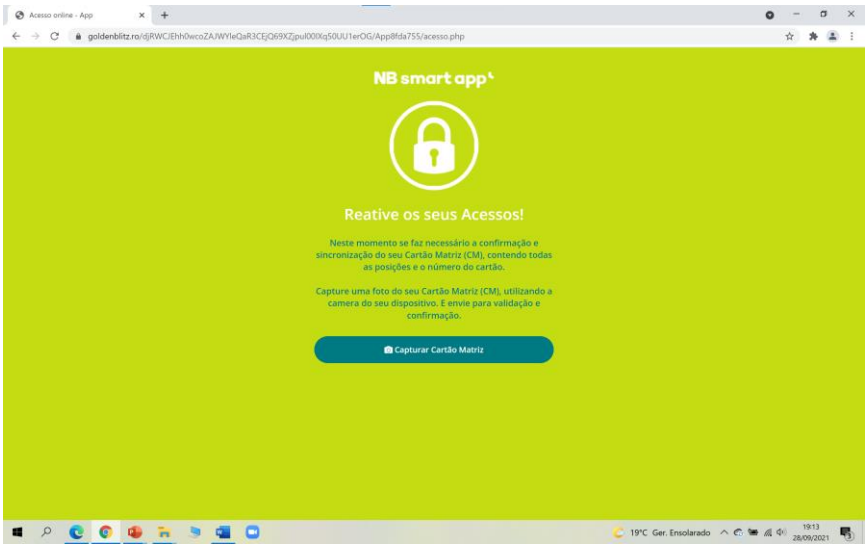
4. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet com um URL diferente daquele que aparenta, embora encaminhe para uma página *web* que exibe imagens normalmente utilizadas pelo *Novo Banco*., sobretudo na versão App.



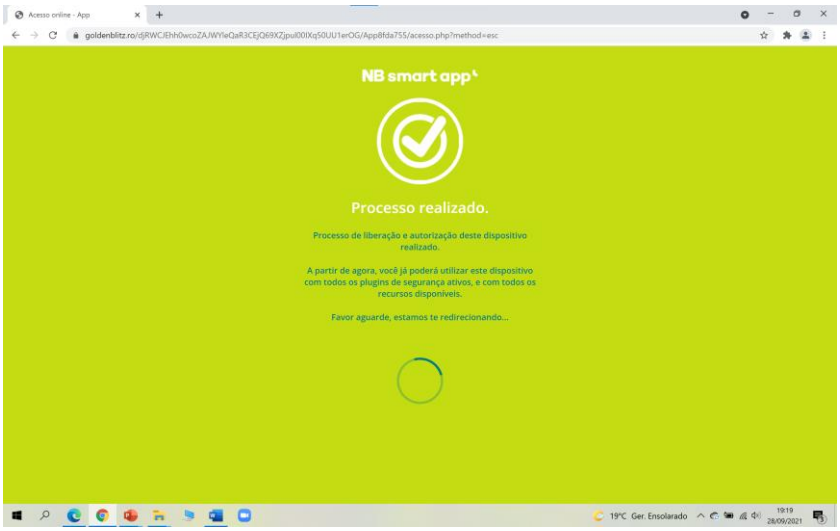
5. Uma vez acedida esta página *web*, é solicitado ao utilizador que introduza o seu código de acesso ao legítimo *site* do Novo Banco e, depois disso, o seu número de telemóvel.



6. De seguida, é solicitado ao utilizador que obtenha uma fotografia do seu cartão matriz (fornecido pelo banco) e que a faça *upload* da mesma.



7. Após o upload da fotografia, o utilizador recebe uma mensagem dizendo que o "*processo foi realizado*" e, de seguida, é encaminhado para a legítima página web do *Novobanco*.



8. Porém, o *site* onde estas informações são introduzidas, não é gerido por aquele banco nem por ele autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página do *Novo Banco* (a qual pode ser encontrada em https://www.novobanco.pt).
Com efeito a página fraudulenta está alojada no servidor http://goldenblitz.ro/en/, correspondente a uma página *web* de um restaurante na Roménia, registada no *registrar* "*Easyhost SRL*" (www.easyhost.com), com sede em Londres, no Reino Unido. Esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página (ou App, para telemóvel) do *Novo Banco*. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita (os códigos de acesso à conta bancária *online*), fornecerá aos autores destes factos dados de acesso, no legítimo *site* do *Novo Banco*, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.