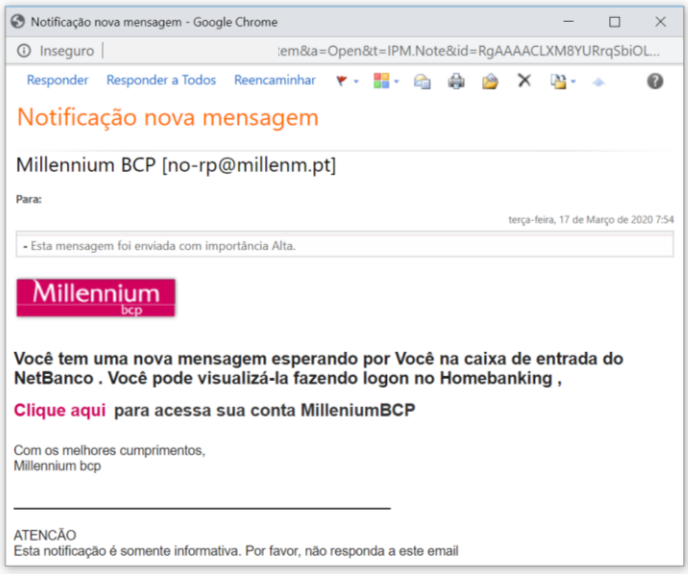
ALERTA CIBERCRIME

17 de março de 2020

'*Phishing*' dirigido a clientes do Millennium BCP

1. Está em curso uma campanha de "*phishing*", dirigida a clientes do banco *Millennium BCP*. 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 recebida a 17 de março às 8 horas e 7 minutos.

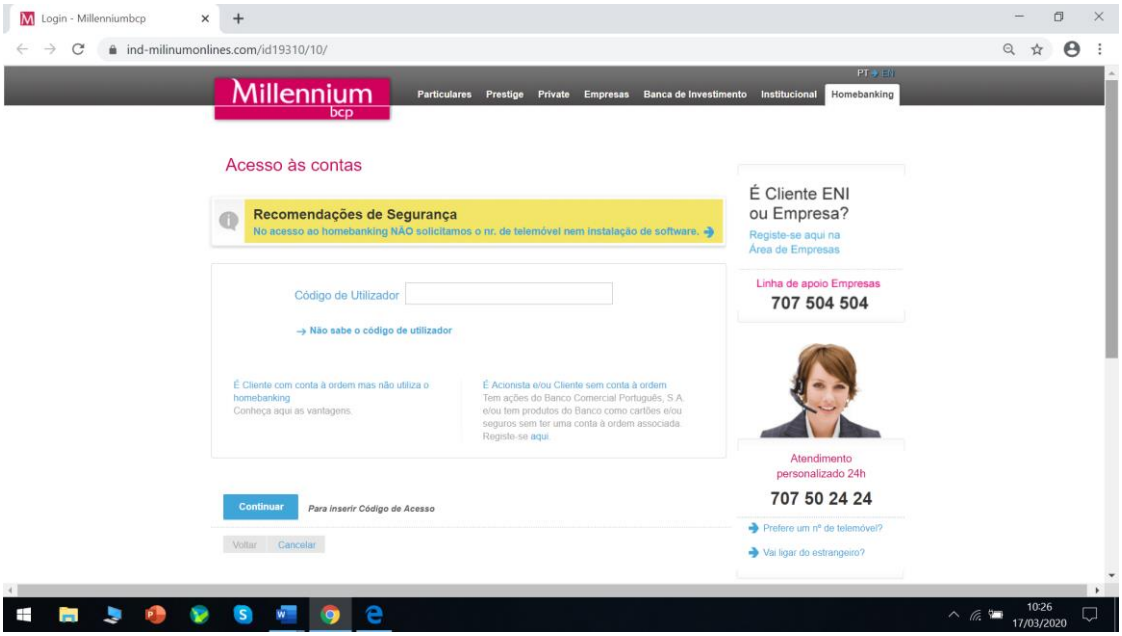
2. Nestas mensagens, com título, no assunto, "*Notificação nova mensagem*" e exibindo-se um logotipo como aquele que é normalmente usado pelo banco *Millennium BCP*, anuncia-se que "*Você tem uma nova mensagem esperando por Você na caixa de entrada do NetBanco. Você pode visualizá-la fazendo logon no Homebanking*".
Além disso, apela-se a que o destinatário "*Clique aqui para acessa sua conta MilleniumBCP*"
As mensagens vêm assinadas com a expressão "*Millennium bcp*".



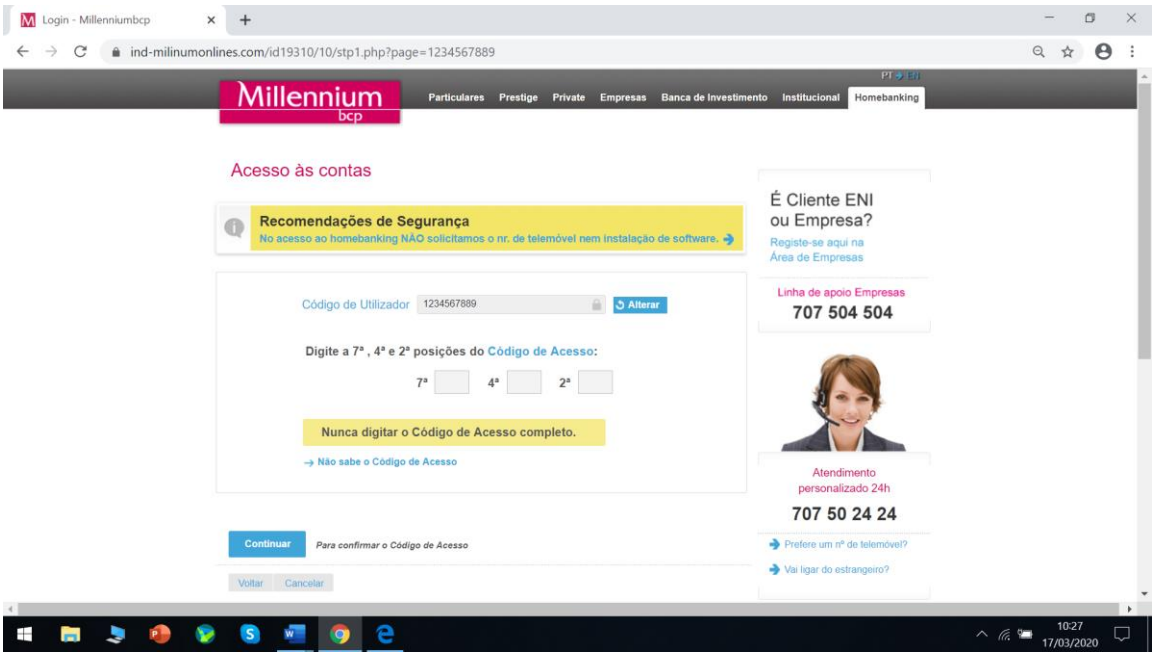
3. Estas mensagens são fraudulentas e não são provenientes do banco *Millennium BCP*. Não foram remetidas pelo banco *Millennium BCP*, nem a partir de sistemas informáticos pertencentes ao mesmo. Aparentemente, tais mensagens foram remetidas a partir do endereço "Millennium BCP" [no-rp@millenm.pt], mas na verdade este endereço de correio eletrónico pertence ao servidor "*Hetzner Online GmbH*" (https://www.hetzner.com), um fornecedor de serviços na *cloud* baseado na Alemanha.

A concreta mensagem identificada pelo Gabinete Cibercrime teve origem num endereço de IP pertencente a "*Digital Ocean, LLC*" (http://www.digitalocean.com) um outro fornecedor de serviços na *cloud*, com sede em Nova Iorque, Estados Unidos da América.

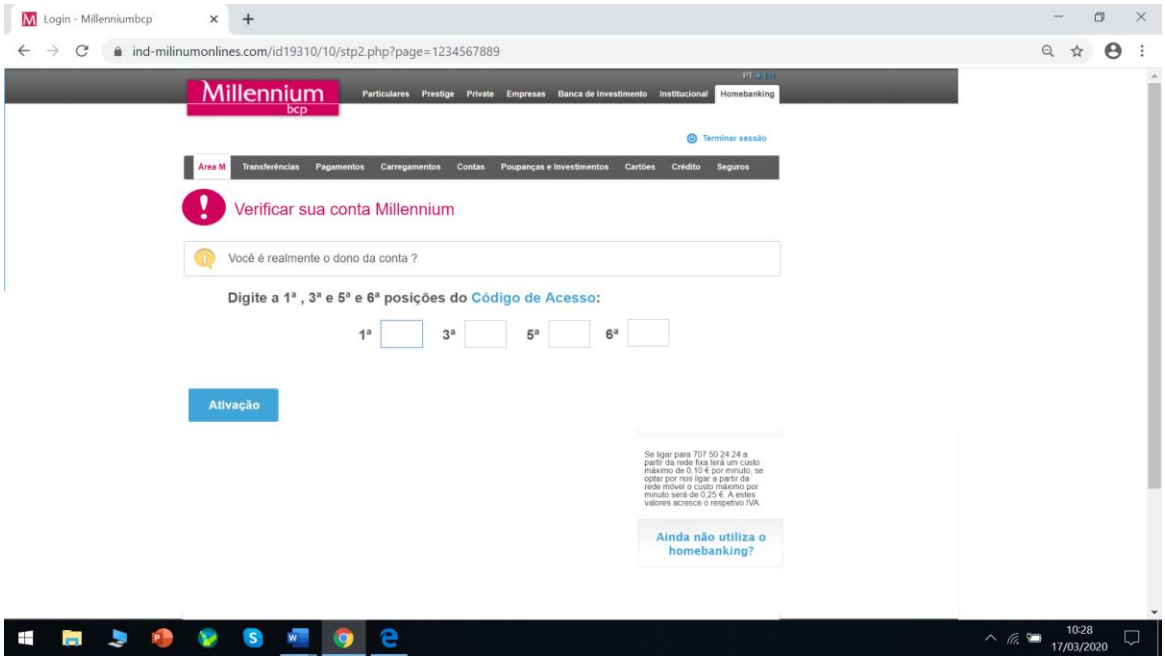
4. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet que aparenta ser o do banco *Millennium BCP*, exibindo imagens gráficas e logotipos normalmente utilizados por aquele banco. Além disso, inclui um espaço em que se solicita a introdução das credenciais de acesso a contas bancárias no banco *Millennium BCP* (pelo serviço de *homebanking*).



Caso o utilizador introduza, como solicitado, o "*Código de Utilizador*", abre-se uma nova página em que é solicitada a introdução de alguns dos dígitos do "*Código de Acesso*".



Sendo introduzidos estes últimos, é perguntado ao utilizador se "*Você é realmente o dono da conta*?" e solicitada a introdução dos restantes dígitos do "*Código de Acesso*".



5. Porém, este *site* não é gerido pelo banco *Millennium BCP* nem é por ele autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página do banco *Millennium BCP*. Tem como único propósito capturar credenciais de acesso *online* a contas de clientes desta instituição bancária.
Esta página fraudulenta está registada no *registrar* "*Name.com, Inc.*", especializado no fornecimento, *online*, de nomes de domínio e outros serviços de Internet, com sede em San Francisco, nos Estados Unidos da América. Aquele domínio fraudulento foi registado a 17 de março de 2020, à 1 hora e 24 minutos.

6. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página do banco *Millennium BCP*. 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 banco *Millennium BCP*, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.