ALERTA CIBERCRIME

2 de setembro de 2017

'*Phishing*' dirigido a clientes do Millenium BCP

1. Está em curso uma campanha de "*phishing*", dirigido a clientes do banco Millenium BCP.

2. Como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. As mensagens desta campanha sinalizadas pelo Gabinete Cibercrime foram recebidas a partir de 24 de agosto de 2017.
Nestas mensagens anuncia-se estar pendente de abertura uma mensagem do banco, a qual é possível aceder por via de um link incluído na mensagem.
Tratam-se, evidentemente, de mensagens fraudulentas, não provenientes do banco Millenium BCP.

3. As mensagens sinalizadas eram insidiosas, uma vez que indicavam serem provenientes do endereço da própria "vítima". Ou seja, o destinatário da mensagem não lograva identificar quem remeteu a mensagem, uma vez que nela figurava, como remetente, o próprio.
Por razões técnicas não foi possível apurar os endereços de IP dos servidores de onde provieram essas mensagens.

4. Os links que se referiram, contidos nas mensagens fraudulentas, conduziam a um s*ite* Internet onde se reproduzem, de forma muitíssimo fiel, todos os conteúdos disponibilizados no *site* autêntico do banco Millenium BCP. Porém, tal *site* não é gerido por aquele banco nem por ele autorizado. A esta página falsa, clonada da página do banco Millenium BCP, corresponde o URL http://www.opticagermana.com/galeria_01/Gallery1/MillenniumBCP/, registado num *registrar*[1] norte-americano (*Domain Central Australia Pty Ltd*) com sede em Maryland e alojado no fornecedor de serviços *Privacy Protect, LLC* (http://privacyprotect.org), igualmente baseado nos EUA, especializado no fornecimento de serviços de computação em nuvem, com anonimato.

5. Recorda-se que a autêntica página do Millenium BCP, está alojada em https://ind.millenniumbcp.pt. Porém, a página fraudulenta é muitíssimo parecida, praticamente igual em aparência, aos olhos do utilizador comum, com a autêntica página do Millenium BCP. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos dados de acesso, no legítimo *site* do Millenium BCP, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.

[1] Um *registrar* é uma organização credenciada para vender, ao público, nomes de domínio.