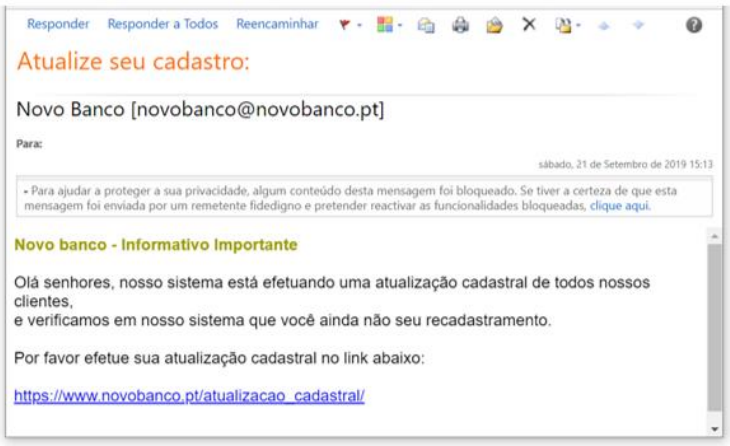
ALERTA CIBERCRIME

23 de setembro de 2019

'*Phishing*' dirigido a clientes do Novobanco

1. Está em curso uma campanha de "*phishing*", dirigida a clientes do banco *Novo Banco*. 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 21 de setembro de 2019, às 15 horas e 14 minutos.

2. Nestas mensagens, com título, no assunto, "A*tualize seu cadastro*" anuncia-se que o banco *Novo Banco* está "*efetuando uma atualização cadastral de todos nossos clientes, e verificamos em nosso sistema que você ainda não seu recadastramento*". Além disso, apela-se a que o destinatário "*efetue sua atualização cadastral no* link *abaixo*". É indicado, para o efeito, o *link* https://www.novobanco.pt/atualizacao_cadastral/.


Responder Responder a Todos Reencaminhar

Atualize seu cadastro:

Novo Banco [novobanco@novobanco.pt]

Para:

sábado, 21 de Setembro de 2019 15:13

- Para ajudar a proteger a sua privacidade, algum conteúdo desta mensagem foi bloqueado. Se tiver a certeza de que esta mensagem foi enviada por um remetente fidedigno e pretender reactivar as funcionalidades bloqueadas, clique aqui.

Novo banco - Informativo Importante

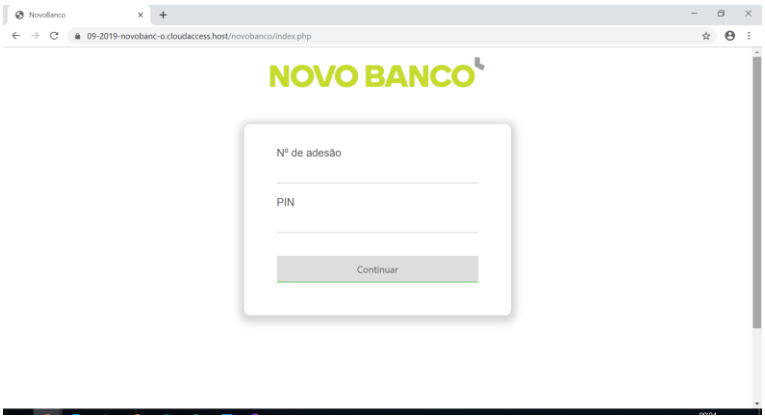
Olá senhores, nosso sistema está efetuando uma atualização cadastral de todos nossos clientes,
e verificamos em nosso sistema que você ainda não seu recadastramento.

Por favor efetue sua atualização cadastral no link abaixo:

https://www.novobanco.pt/atualizacao_cadastral/

3. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do banco *Novo Banco*. Não foram remetidas pelo *Novo Banco* nem a partir de sistemas informáticos pertencentes ao mesmo.
Na verdade, provieram de um servidor de *email*, que usou o endereço de IP 170.78.75/24, pertencente à empresa argentina *BAEHOST* (https://baehost.com/en-int/), um fornecedor de serviços da "*cloud*", com servidores localizados em Buenos Aires, na Virgínia e Florida (Estados Unidos da América), no Canadá e em França (https://baehost.com/en-int/empresa/datacenter).

4. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduzia a um *site* Internet com um URL diferente daquele que aparentava, o qual exibia imagens normalmente utilizadas pelo banco *Novo Banco*.



5. Porém, tal *site* não é gerido por aquele banco nem por ele autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página do banco *Novo Banco* (a qual pode ser encontrada em https://www.novobanco.pt).

A página fraudulenta está alojada no servidor *Cloud Access LLC* (https://www.cloudaccess.net), um fornecedor de serviços da "*cloud*", sedeado no Estado do Michigan, nos Estados Unidos da América. Pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página do banco *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 banco *Novo Banco*, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.

Aliás, quando é introduzida informação na página não autêntica, de forma fraudulenta é emitida a informação de que "*seu cadastro foi atualizado com sucesso*!!!". Também esta informação não é providenciada pelo banco *Novo Banco*.