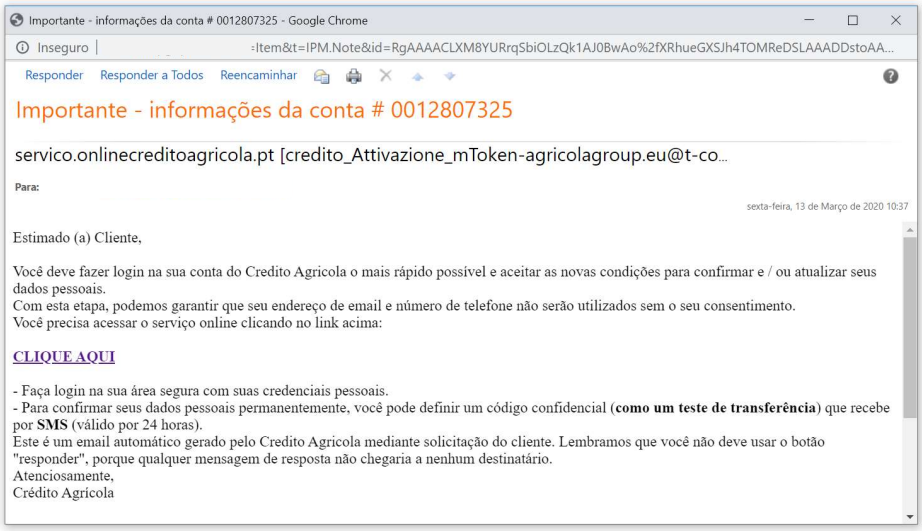
ALERTA CIBERCRIME

13 de março de 2020

'*Phishing*' dirigido a clientes do Crédito Agrícola

1. Está em curso uma campanha de *phishing*, dirigida a clientes da instituição bancária *Crédito Agrícola*. 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 13 de março de 2020, pelas 10 horas e 37 minutos.

2. Nestas mensagens, com o título, no assunto, "*Importante – informações da conta # 0012807325*" anuncia-se que o destinatário da mensagem "*deve fazer login na conta do Crédito Agrícola o mais rápido possível e aceitar as novas condições para confirmar e/ou atualizar seus dados pessoais*." Indica-se de seguida um *link*, assinalado com a expressão "*CLIQUE AQUI*". As mensagens vêm assinadas com a expressão "*Crédito Agrícola*".


Importante - informações da conta # 0012807325 - Google Chrome

Inseguro | -Item&t=IPM.Note&id=RgAAAACLXM8YURrqSbiOLzQk1AJ0BwAo%2fXRhueGXSJh4TOMReDSLAAADDstoAA...

Responder Responder a Todos Reencaminhar

Importante - informações da conta # 0012807325

servico.onlinecreditoagricola.pt [credito_Attivazione_mToken-agricolagroup.eu@t-co...

Para:

sexta-feira, 13 de Março de 2020 10:37

Estimado (a) Cliente,

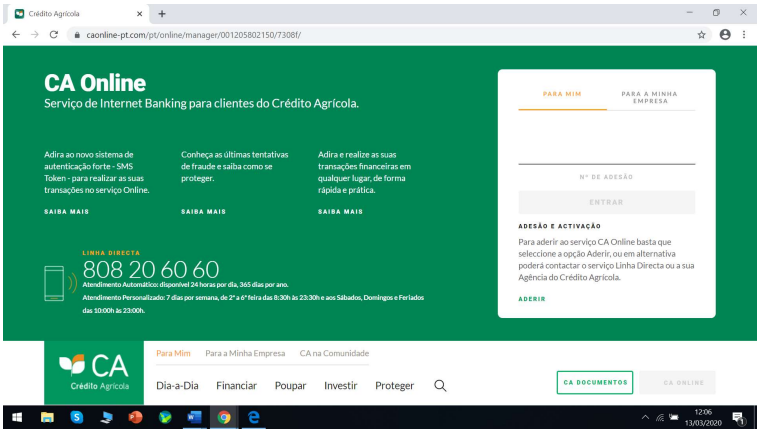
Você deve fazer login na sua conta do Credito Agricola o mais rápido possível e aceitar as novas condições para confirmar e / ou atualizar seus dados pessoais.
Com esta etapa, podemos garantir que seu endereço de email e número de telefone não serão utilizados sem o seu consentimento.
Você precisa acessar o serviço online clicando no link acima:

CLIQUE AQUI

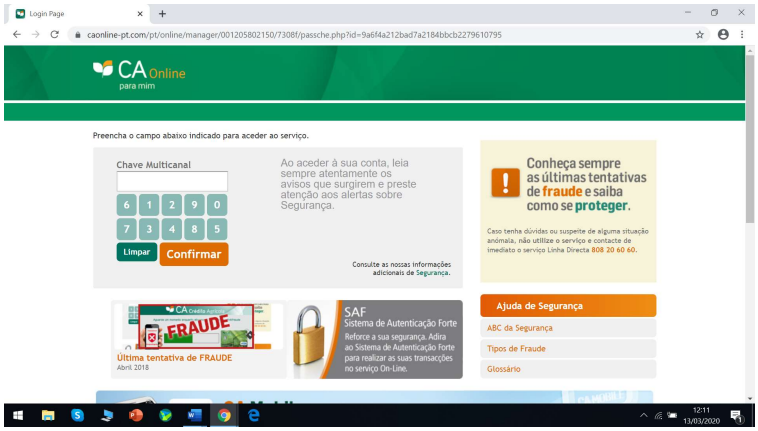
- Faça login na sua área segura com suas credenciais pessoais.
- Para confirmar seus dados pessoais permanentemente, você pode definir um código confidencial (**como um teste de transferência**) que recebe por **SMS** (válido por 24 horas).
Este é um email automático gerado pelo Credito Agricola mediante solicitação do cliente. Lembramos que você não deve usar o botão "responder", porque qualquer mensagem de resposta não chegaria a nenhum destinatário.
Atenciosamente,
Crédito Agrícola

3. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do *Crédito Agrícola*. Não foram remetidas pelo *Crédito Agrícola* nem a partir de sistemas informáticos pertencentes ao mesmo. Aparentemente, tais mensagens foram remetidas por "serviço.onlinecreditoagricola.pt", mas na verdade provieram do endereço credito_Attivazione_mToken-agricolagroup.eu@t-com.hr, o qual usa os serviços de *webmail* da "*Croatian Telecom Inc*." ("*Hrvatski Telekom d.d.*"), com sede em Draskoviceva 26, HR-10000, em Zagreb, na Croácia.

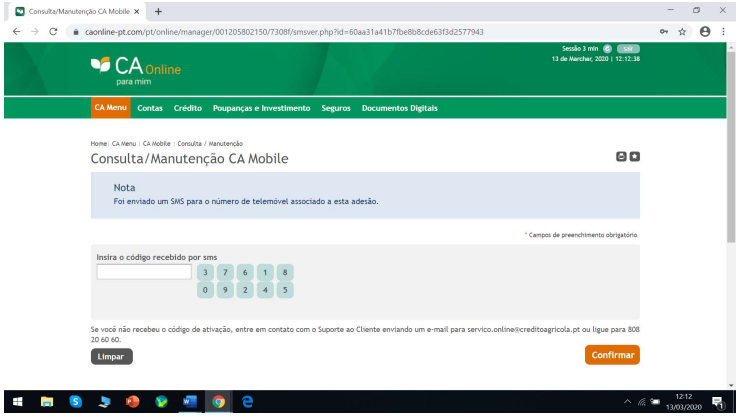
4. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet que aparenta ser o do *Crédito Agrícola*, exibindo imagens gráficas e logotipos normalmente utilizados por aquele. Além disso, inclui um espaço em que se solicita a introdução das credenciais de acesso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



Caso o utilizador introduza, como solicitado, o "*número de adesão*", abre-se uma nova página em que é solicitada a introdução da "*chave multicanal*".



Sendo introduzida esta última, ainda é solicitado que o utilizador introduza um "*código recebido por sms*". Porém, nenhum código é remetido por sms.



5. Este *site* não é gerido pelo *Crédito Agrícola* nem é por ele autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página do *Crédito Agrícola*. Tem como único propósito capturar credenciais de acesso *online* a contas de clientes desta instituição bancária.
Esta página fraudulenta está registada no fornecedor de serviços "*Tucows Domains Inc*." (http://tucowsdomains.com), com sede em Toronto, no Canadá, especializado no fornecimento de nomes de domínio e outros serviços de Internet. Aquele domínio fraudulento foi registado a 12 de março de 2020.

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