MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

27 de setembro de 2018

Phishing – CRÉDITO AGRÍCOLA

1. Chegou, ao Gabinete Cibercrime, nota de que está em curso uma campanha de *phishing* dirigido a titulares de contas bancárias na *Caixa Central de Crédito Agrícola Mútuo* (Crédito Agrícola).
Como habitual em casos desta natureza, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira mensagem desta nova campanha sinalizada pelo Gabinete Cibercrime data de 26 de setembro de 2018, como consta da imagem que segue.

De: CreditoAgricola <comedirectservisupporthsisxcldrll@castillosdesoria.com>
Enviado: 26 de setembro de 2018 17:49
Para:
Assunto: Re

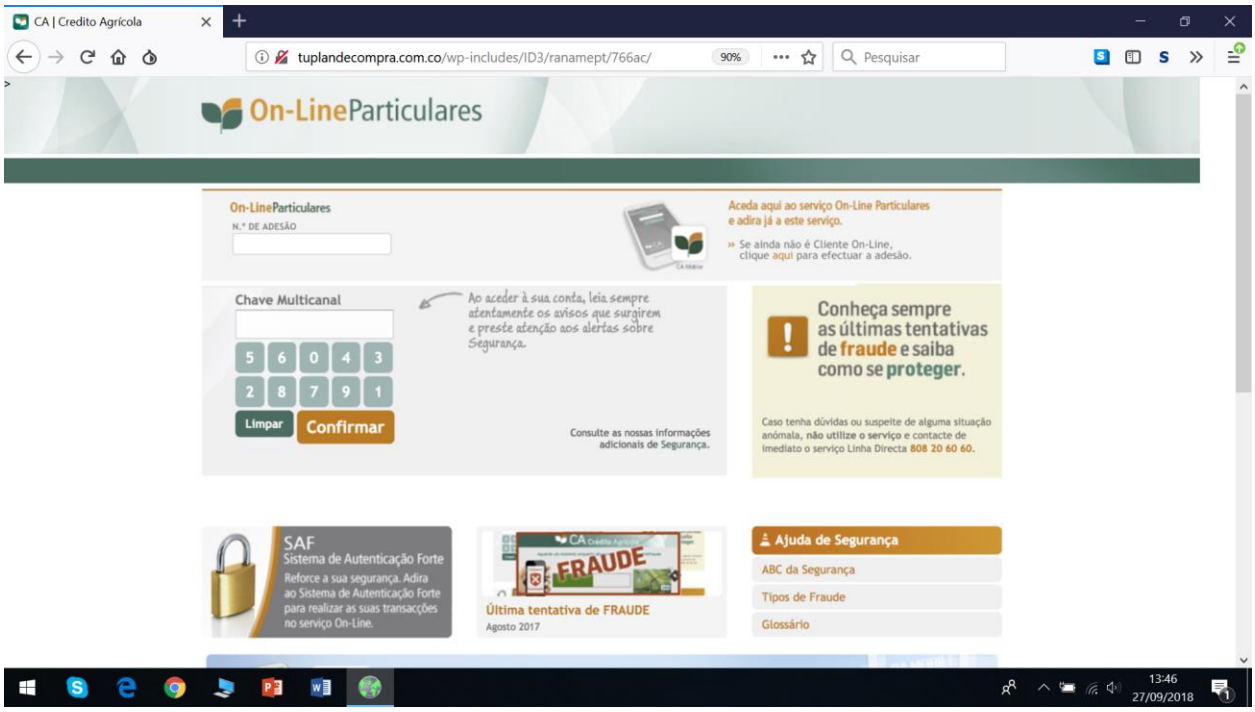
CREDITO AGRICOLA,
Convidamos você a revisar sua conta para atualizar suas informações pessoais.
Para atualizar suas informações de contato, por favor clique no seguinte link:
Atualizar minhas informações
Esta mensagem é gerada automaticamente.

---

2. Supostamente, esta mensagem provinha do endereço comedirectservisupporthsisxcldrll@castillosdesoria.com, mas não foi possível apurar a sua verdadeira origem.

3. Na mensagem, incitava-se o destinatário a "*revisar sua conta para atualizar suas informações pessoais*", indicando-se que tal poderia ser feito acedendo à mesma conta por via de um *link*, incluído na própria mensagem, onde deviam ser introduzidas as credenciais de acesso a conta bancária no Crédito Agrícola.
Esta mensagem é fraudulenta e não teve origem em qualquer serviço do Crédito Agrícola.

4. O *link* indicado na mensagem conduz ao site http://tuplandecompra.com.co/wp-includes/ID3/ranamept/766ac/, no qual se reproduzem conteúdos e imagens aparentemente disponibilizados pelo Crédito Agrícola, como resulta da imagem que segue.



Este *site*, porém, não pertence ao Crédito Agrícola nem é por ele gerido. Trata-se de um *site* cujo domínio pertence ao Registrar Godaddy.com, baseado nos Estados Unidos, vendido por um ano (a 23 de abril de 2018), ao Registrant Pegateya, do qual se sabe apenas que está baseado na província de Santander, na Colômbia.

5. Este *site* fraudulento pretende ser parecido, aos olhos do utilizador comum, com a autêntica página do Crédito Agrícola (alojada em https://www.creditoagricola.pt/). Se a vítima aceder a ele e nele introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados necessários ao acesso, no legítimo *site* do Crédito Agrícola, à sua conta.