

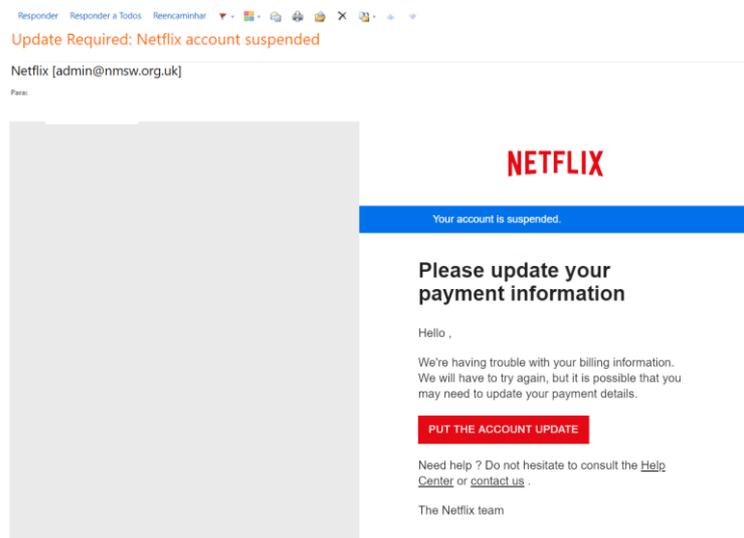


ALERTA CIBERCRIME

19 de dezembro de 2018

Phishing - contas Netflix

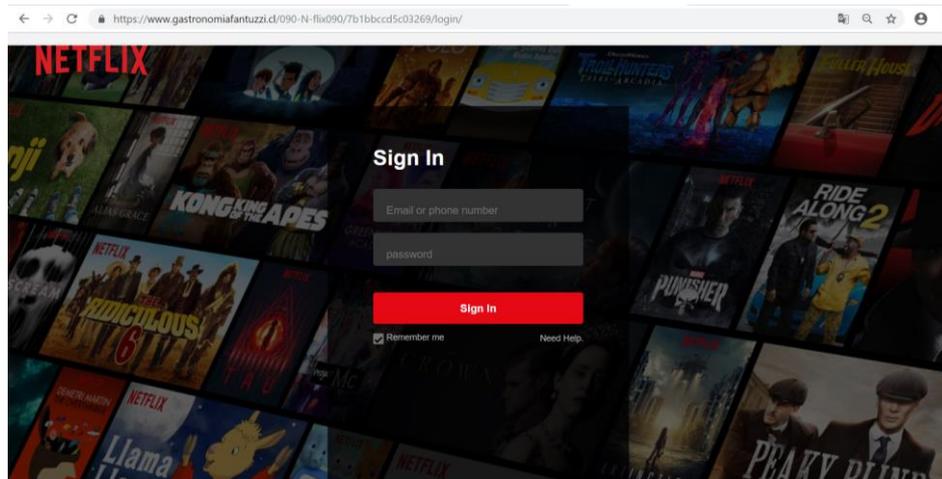
1. Está em curso mais uma campanha de "*phishing*", desta vez dirigida a titulares de contas Netflix. Como habitual em casos desta natureza, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira mensagem desta nova campanha sinalizada pelo Gabinete Cibercrime foi registada às 10 horas e 34 minutos de 19 de dezembro de 2018 e provinha do endereço "Netflix [admin@nmsw.org.uk]". Supostamente, esta mensagem deveria ter tido origem no domínio <http://www.nmsw.org.uk/>, correspondente à página *web* de um projeto educativo na área musical. Porém, na verdade, tal mensagem foi remetida a partir do endereço de IP 185.81.157.165, pertencente ao ISP *Inulogic* (<https://www.inulogic.fr>), com sede em Saint-Priest, França. Este ISP dedica-se, entre outros, a fornecer aos seus clientes alojamento de conteúdos na chamada *cloud*, incluindo por via de servidores VPS (*Virtual Private Server*).



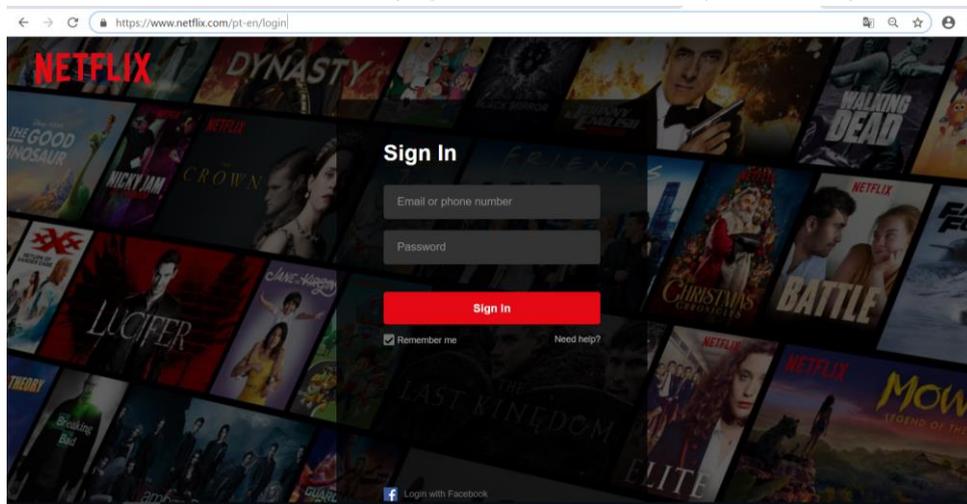
2. Nestas mensagens, assinadas por um suposto "The Netflix team", anuncia-se que a conta Netflix do destinatário está suspensa, sendo necessário proceder a uma atualização da informação respeitante ao pagamento. Depois, incita-se ao acesso ao Netflix, com a expressão "PUT THE ACCOUNT UPDATE". Esta expressão encaminha o utilizador, por via de um *link*. Esta tipo de mensagem é fraudulenta e não teve origem em qualquer serviço da Netflix.



3. Por outro lado, o *link* indicado na mensagem como conduzindo ao verdadeiro site da Netflix, conduz o utilizador para o site <https://www.gastronomiafantuzzi.cl/090-N-flix090/fcf9eecac8605bc/login/>. Quando se acede a este *link*, são exibidos ao utilizador conteúdos iguais aos disponibilizados no site autêntico da Netflix e imagens associadas a esta.



Porém, esta página web não pertence à Netflix nem por ela é gerida (está alojada no espaço de uma entidade com sede no Chile). A verdadeira página da Netflix está alojada em <https://www.netflix.com>.



4. O *link* indicado na mensagem conduz assim a um *site* que, embora muito parecido ao original, aos olhos do utilizador comum, é fraudulento.

Com efeito, se o utilizador aceder a ele e nele introduzir a informação que se lhe solicita, fornecerá aos autores destes factos os dados necessários ao acesso à sua conta., no legítimo *site* da Netflix. São ainda pedidos dados de identificação pessoal e dados do cartão de crédito da vítima, incluído o código de autenticação (CVV).