MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

11 de dezembro de 2017

Phishing - contas Apple

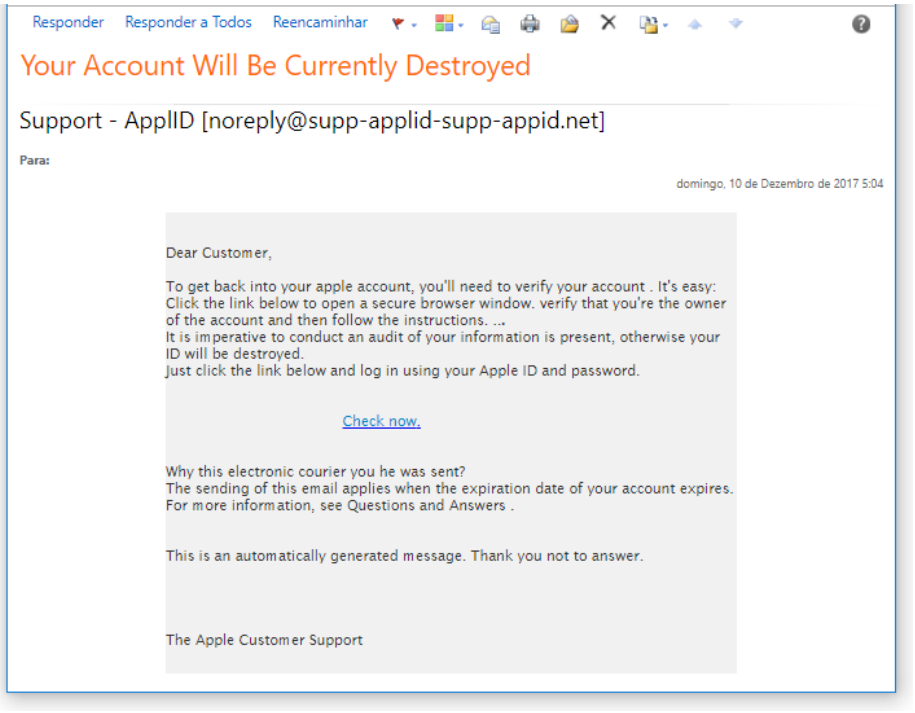
1. Está em curso mais uma campanha de "*phishing*" dirigido a titulares de contas Apple.
Como habitual em casos desta natureza, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. A primeira mensagem desta nova campanha sinalizada pelo Gabinete Cibercrime datava de 10 de dezembro de 2017 e provinha, supostamente, do endereço "ApplID noreply@supp-applid-supp-appid.net" (Anexo 1).
Na verdade, tal mensagem foi remetida a partir de uma conta de correio eletrónico de um servidor baseado na Alemanha (www.strato.de, pertencente à sociedade "Strato AG", com sede em Berlim) o qual permite a aquisição, *online*, de contas de correio com domínio personalizado (portanto, escolhido pelo utilizador).

2. Nestas mensagens, assinadas por um "*The Apple Customer Support*", anuncia-se estar prestes a ser "destruída" a conta Apple do destinatário ("*Your Account Will Be Currently Destroyed*"). Esta *destruição* apenas se evitará se o destinatário verificar a sua conta, acedendo à mesma, por via de um *link* incluído na própria mensagem, onde devem ser introduzidas as credenciais de acesso à loja Apple.
Estas mensagens são fraudulentas e não tiveram origem em qualquer serviço da Apple.

3. O *link* indicado na mensagem conduz ao *site* https://ppsecure-servicessl-sessionid2615653002tt.do-inuserid.org/kym (Anexo 2), no qual se reproduzem conteúdos disponibilizados no *site* autêntico da Apple e imagens associadas a esta.
Este *site*, porém, não pertence à Apple nem por ela é gerido. Trata-se de um *site* cujo domínio fora adquirido dias antes da remessa das mensagens (a 4 de dezembro de 2017) ao *registrar* "Cronon AG" (http://www.cronon.net), um prestador de serviços da *cloud*, baseado na Alemanha. O registo de um domínio, bem como o pagamento do mesmo, neste prestador de serviços da *cloud* pode ser feito *online*, a partir de qualquer parte do mundo.

4. Este *site* fraudulento é muito parecido, aos olhos do utilizador comum, com a autêntica página da Apple. 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* da Apple, à sua conta.

ANEXO 1



Responder Responder a Todos Reencaminhar

Your Account Will Be Currently Destroyed

Support - AppIID [noreply@supp-applid-supp-appid.net]

Para:

domingo, 10 de Dezembro de 2017 5:04

Dear Customer,

To get back into your apple account, you'll need to verify your account . It's easy:
Click the link below to open a secure browser window. verify that you're the owner of the account and then follow the instructions. ...
It is imperative to conduct an audit of your information is present, otherwise your ID will be destroyed.
Just click the link below and log in using your Apple ID and password.

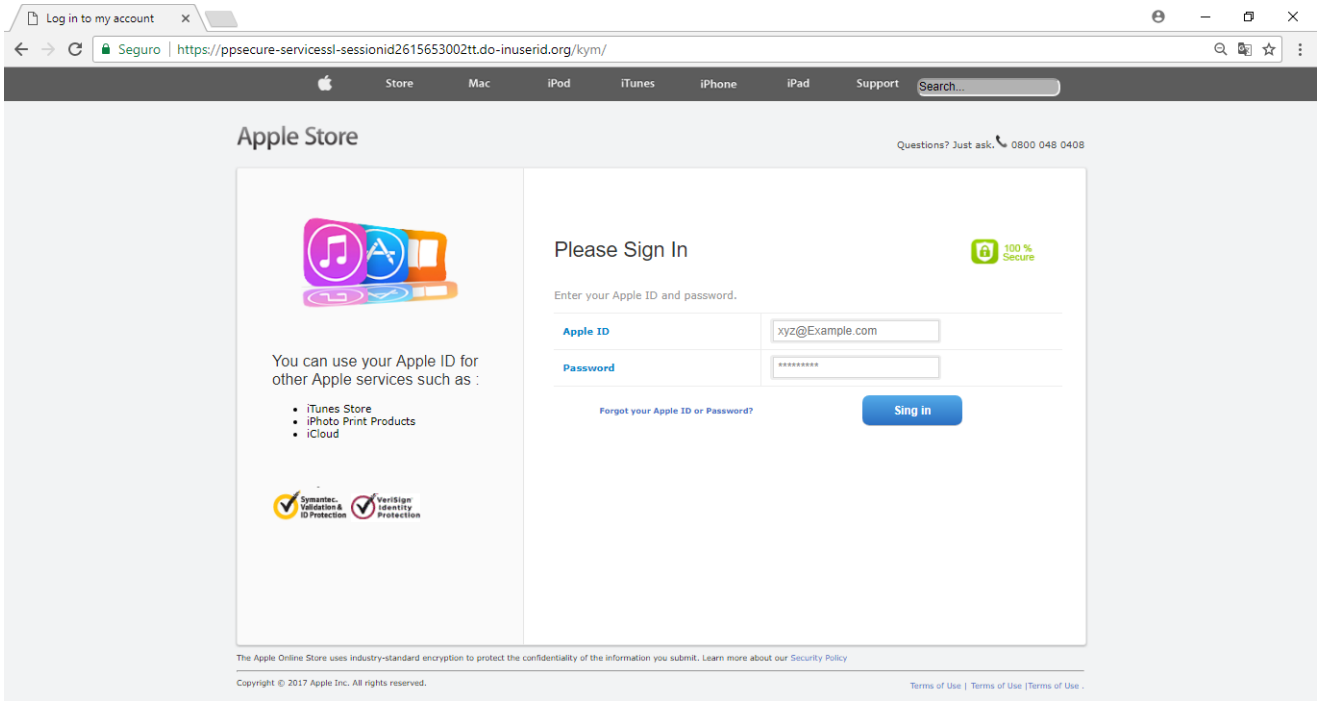
Check now.

Why this electronic courier you he was sent?
The sending of this email applies when the expiration date of your account expires.
For more information, see Questions and Answers .

This is an automatically generated message. Thank you not to answer.

The Apple Customer Support

ANEXO 2



Log in to my account

Seguro | https://ppsecure-servicessl-sessionid2615653002tt.do-inuserid.org/kym/

Store Mac iPod iTunes iPhone iPad Support Search...

Apple Store

Questions? Just ask. 0800 048 0408

Please Sign In

100 % Secure

Enter your Apple ID and password.

Apple ID xyz@Example.com

Password

Forgot your Apple ID or Password?

Sing in

You can use your Apple ID for other Apple services such as :

- iTunes Store
- iPhoto Print Products
- iCloud

Symantec. Validation & ID Protection VeriSign Identity Protection

The Apple Online Store uses industry-standard encryption to protect the confidentiality of the information you submit. Learn more about our Security Policy

Copyright © 2017 Apple Inc. All rights reserved.

Terms of Use | Terms of Use | Terms of Use .