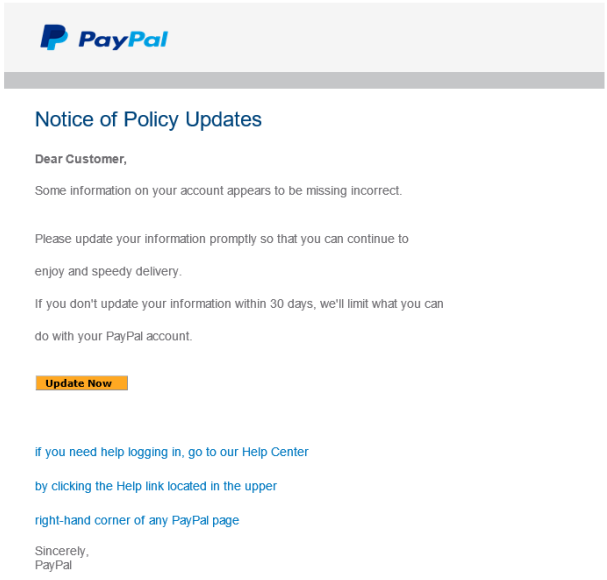
ALERTA CIBERCRIME

16 de outubro de 2018

Phishing – PAYPAL

1. Chegou, ao Gabinete Cibercrime, nota de que está em curso uma campanha de *phishing* dirigido a titulares de contas no prestador de serviços *online* Paypal (https://www.paypal.com).
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 16 de outubro de 2018 e tem o teor da imagem que segue.


PayPal

Notice of Policy Updates

Dear Customer,

Some information on your account appears to be missing incorrect.

Please update your information promptly so that you can continue to enjoy and speedy delivery.

If you don't update your information within 30 days, we'll limit what you can do with your PayPal account.

Update Now

if you need help logging in, go to our Help Center by clicking the Help link located in the upper right-hand corner of any PayPal page

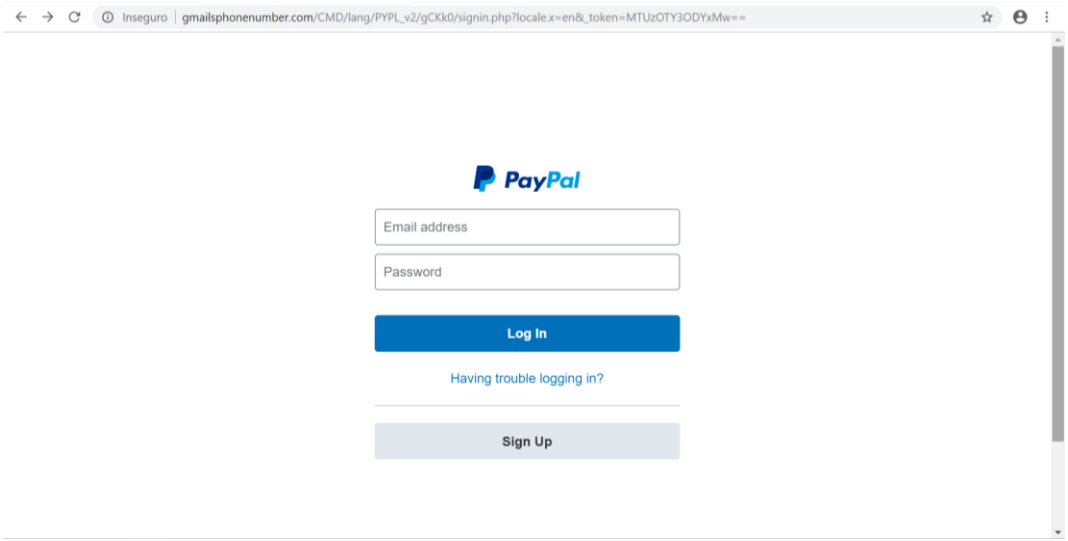
Sincerely,
PayPal

2. Esta mensagem provinha do endereço info@ded3497.inmotionhosting.com, que se arroga pertencer ao PayPal, o que não é verdade. Com efeito, este endereço de *email* foi disponibilizado pelo fornecedor de serviços *web* "InMotion Hosting Inc" (https://www.inmotionhosting.com), com sede em El Segundo, na Califórnia, Estados Unidos da América. Trata-se de um fornecedor de serviços que vende *online* alojamento de *sites*, incluindo *webmail*.

3. Todavia, embora tenha utilizado os serviços e um endereço de IP (23.235.222.235) pertencente à "InMotion Hosting Inc", na verdade, a mensagem proveio de um servidor alojado no endereço www.server.xsited.com, baseado em Phnom Penh, no Camboja.

4. A mensagem incita o destinatário a atualizar a informação sobre a respetiva conta no Paypal, sob pena de, não o fazendo, a utilização dessa mesma conta vir a ser limitada. Além disso, disponibiliza um botão, conduzindo a um *link* supostamente pertencente à página *web* do Paypal.

5. Este *link* não conduz a qualquer página do Paypal, antes direcionando o utilizador para o *site* http://gmailsphonenumber.com/CMD/lang/PYPL_v2/gCKk0/signin.php?locale.x=en&_token=MTUzOTY3ODYxMw. Neste *site* reproduzem-se sinais identificativos, conteúdos e imagens aparentemente pertencente ao PayPal, pretendendo fazer crer quem o aceda que se trata do verdadeiro *site* daquele fornecedor de serviço, como resulta da imagem que segue.



6. Acedido o *site*, é solicitado ao utilizador que introduza os seus códigos de acesso ao serviço Paypal, sendo de seguida o utilizador informado de que a sua conta foi recentemente acedida, a partir de um local nos Estados Unidos. Depois é solicitada a introdução de diversa outra informação: todos os dados do cartão de crédito, os dados de acesso à conta bancária e cópia de um documento de identificação do utilizador.
Uma vez introduzidos todos estes dados, o utilizador é informado de que a conta foi restaurada e encaminhado para a legítima página do Paypal na Internet (https://www.paypal.com/pt/home).

7. Porém, este *site* não pertence ao Paypal nem é por ele gerido. Trata-se de um domínio alojado no fornecedor de serviço "Hetzner Online GmbH" (https://www.hetzner.com), com sede em Gunzenhausen, na Alemanha, o qual se dedica à venda *online*, entre outras, de páginas *web*.