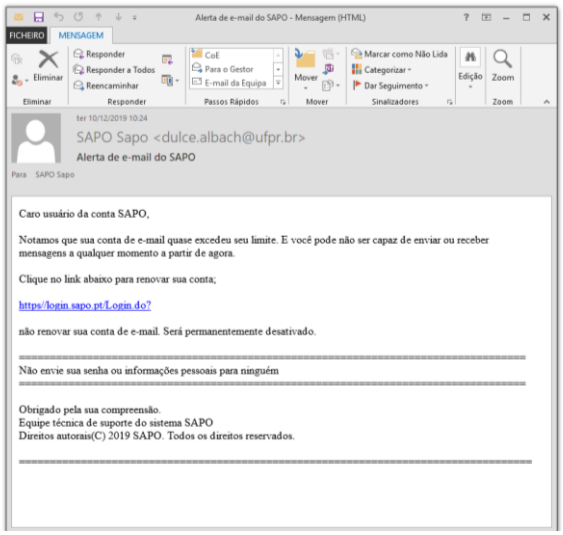
ALERTA CIBERCRIME

10 de dezembro de 2019

Phishing – Serviço de *Webmail* SAPO

1. Está em curso uma campanha de *phishing*, pela qual os seus agentes pretendem obter ilegitimamente credenciais de acesso a contas de correio eletrónico do serviço de *webmail* SAPO. Como é habitual em campanhas de *phishing*, o processo teve início com a remessa, para as vítimas, de mensagens de correio eletrónico com conteúdo enganador.

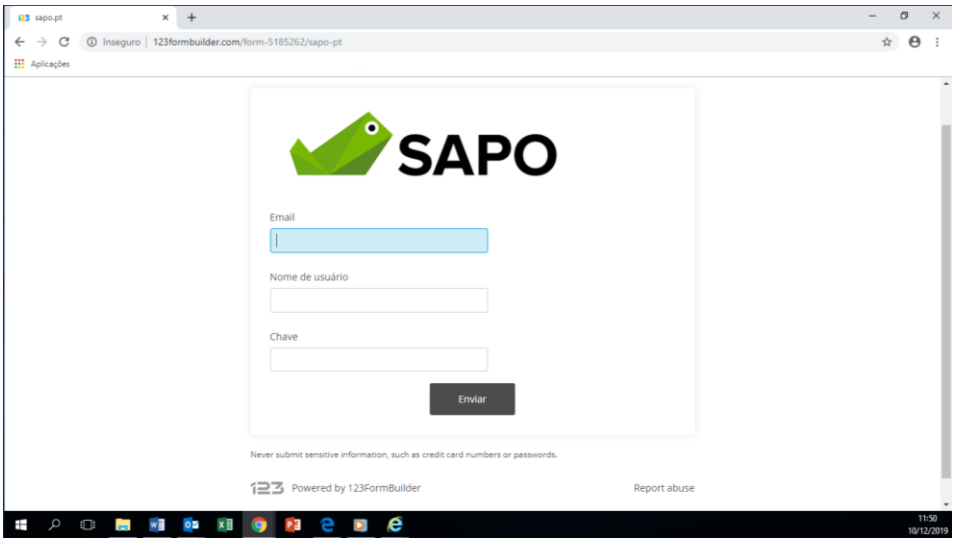
2. Em concreto caso identificado pelo Gabinete Cibercrime, a mensagem foi expedida a 10 de dezembro de 2019, às 10 horas e 24 minutos, pela conta de *email* dulce.albach@ufpr.br. Trata-se de uma mensagem proveniente de uma conta de correio eletrónico legítima, pertencente a uma colaboradora da Universidade Federal do Paraná, no Brasil (http://correio.ufpr.br). Todavia, suspeita-se que o acesso a esta conta (efetuado quando no Brasil eram um pouco mais que as 7 horas da manhã) tenha sido feito de forma ilegítima.



3. A mensagem de *phishing* identificada vinha assinada por uma suposta "*Equipe técnica de suporte do sistema SAPO*" e, dirigindo-se a um suposto "*usuário da conta SAPO*", referia que "*notamos que sua conta de e-mail quase excedeu seu limite. E você pode não ser capaz de enviar ou receber mensagens a qualquer momento a partir de agora.*" Ainda apelava para que o destinatário acedesse a um *link* para "*renovar*

sua conta". Ainda advertia que a não *renovação* da conta tinha como consequência que "*será permanentemente desativada*".

4. Quanto ao *link*, visualmente vinha indicado como https//login.sapo.pt/Login.do?. A verdade, porém, é que quando acedido, encaminhava o utilizador para a página *web* http://www.123formbuilder.com/form-5185262/sapo-pt.



Esta página, quando aberta, exibe ao utilizador uma imagem gráfica parecida à que é utilizada pelo legítimo serviço de *Webmail* SAPO, pedindo ao utilizador que nela introduza o seu "*Email*", "*Nome de usuário*" e "*Chave*".

5. Porém, a mensagem fraudulenta não foi remetida pelo serviço de *webmail* SAPO. Por outro lado, a página *web* em causa também não corresponde a nenhuma forma de acesso *online* ao serviço de correio eletrónico SAPO.
Assim, o conteúdo da página é enganador. Não permite o acesso a qualquer conta de correio eletrónico e pretende apenas convencer o utilizador a facultar as credenciais de acesso à sua legítima conta de correio eletrónico.

6. Na verdade, a página em causa está alojada no fornecedor de serviço https://www.123formbuilder.com, com sede na Roménia, o qual é especializado no fornecimento de formulários para utilização *online*. Para a utilização deste serviço, é apenas necessário que o utilizador esteja munido de um qualquer endereço de correio eletrónico e crie uma conta *online*. Este modelo de exploração permite, pois, o uso totalmente anonimizado do serviço.