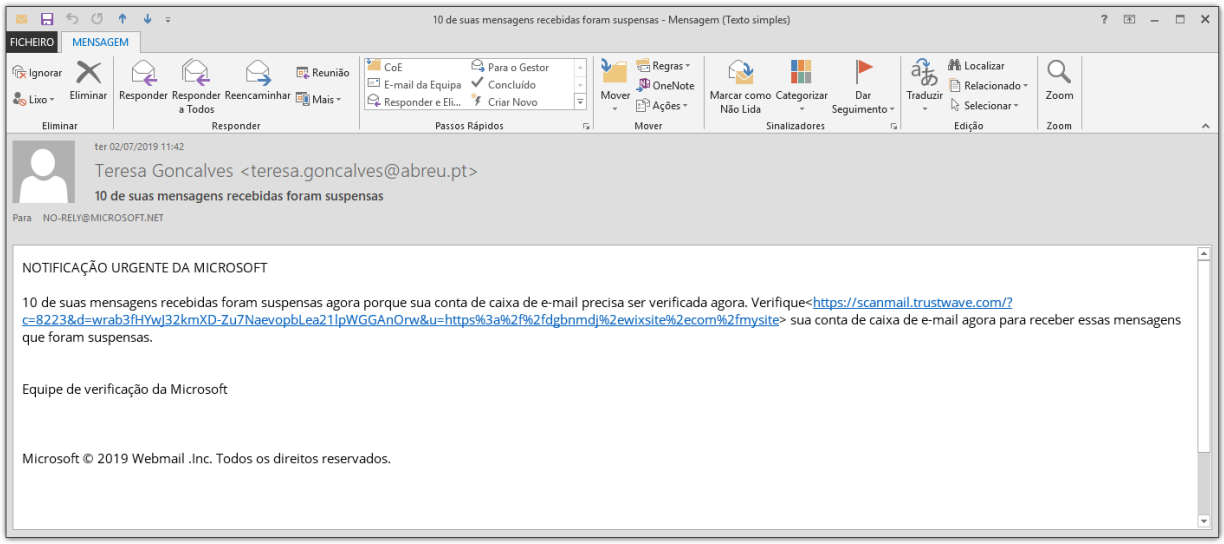
ALERTA CIBERCRIME

2 de julho de 2019

Phishing – Passwords de Correio Eletrónico *(Outlook Web)*

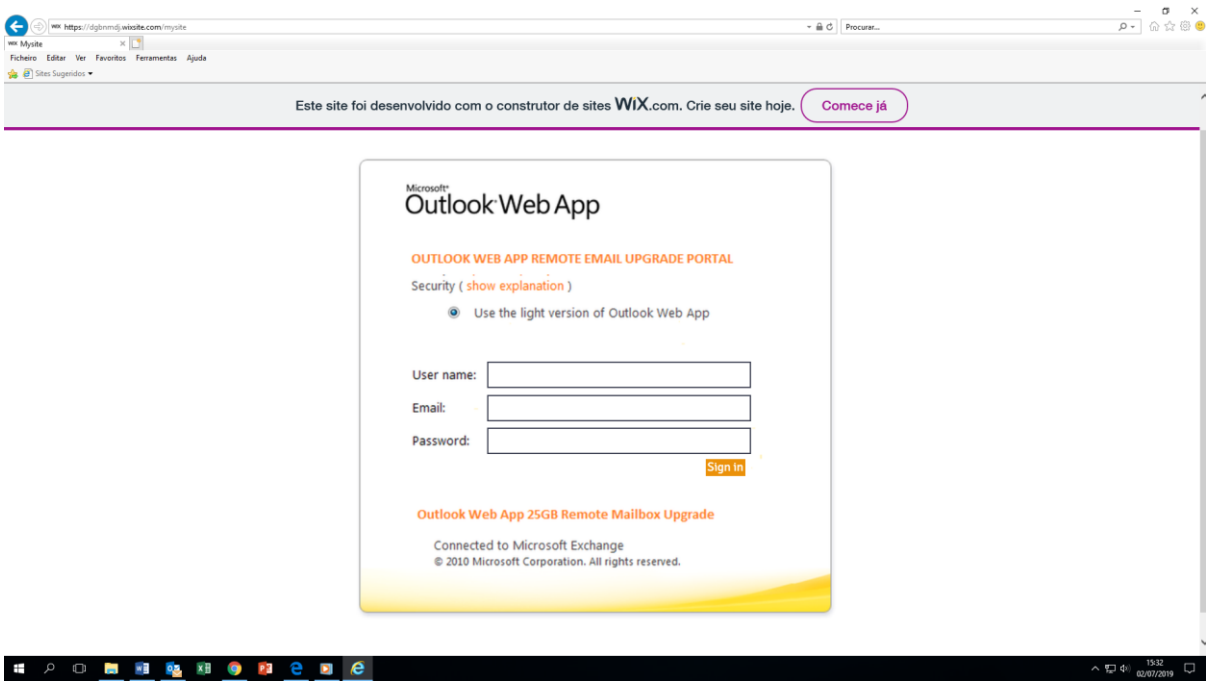
1. Está em curso uma campanha de *phishing* pela qual os seus agentes pretendem obter ilegitimamente credenciais de acesso a contas de correio eletrónico. Como é habitual em campanhas de *phishing*, o processo tem início com a remessa, para as potenciais vítimas, de mensagens de correio eletrónico com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

2. Em concreto caso identificado pelo Gabinete Cibercrime, a mensagem foi expedida a 2 de julho de 2019, às 11 horas e 42 minutos, por desconhecido que usou a conta de *email* teresa.goncalves@abreu.pt. Trata-se de uma mensagem proveniente de uma conta de correio eletrónico pertencente a um domínio de uma sociedade comercial portuguesa, suspeitando-se que terá havido ilegítimo acesso à mesma, para ulterior expedição da mensagem em causa.



3. A mensagem de *phishing* vinha assinada por uma suposta "*Equipe de verificação da Microsoft*" e, assumindo como "assunto" o de "*10 de suas mensagens recebidas foram suspensas*", referia, sob a epígrafe *NOTIFICAÇÃO URGENTE DA MICROSOFT* que "*10 de suas mensagens recebidas foram suspensas agora porque sua conta de caixa de e-mail precisa ser verificada agora*". Ainda apelava para que o

destinatário acedesse a um *link* para que aí verificasse "*sua conta de caixa de e-mail agora para receber essas mensagens que foram suspensas*".
Este *link*, se acedido, dirigia o utilizador para a página *web* https://dgbnmdj.wixsite.com/mysite. Esta página, quando aberta, exibe ao utilizador uma imagem gráfica parecida à que é utilizada pela aplicação *Outlook Web App*, usada para aceder a correio eletrónico de forma remota. Sobre a mesma, inscrições em inglês apelam à inserção do nome de utilizador, do endereço de correio eletrónico e da senha de acesso à conta.



5. Porém, a mensagem fraudulenta não foi remetida por nenhum serviço da sociedade Microsoft. Por outro lado, a página *web* em causa também não corresponde a nenhum serviço *online* de acesso a correio eletrónico de qualquer entidade cliente da Microsoft.
Na verdade, a página em causa está alojada no fornecedor de serviço www.wix.com, com origem nos Estados Unidos da América e especializado em serviços de alojamento na chamada *cloud* (sobretudo o alojamento remoto de *sites*), o qual garante proteção dos dados de identidade dos seus clientes.
O seu conteúdo é enganador. Não permite o acesso a qualquer conta de correio eletrónico e pretende apenas convencer o utilizador a facultar a desconhecidos as credenciais de acesso à sua legítima conta de correio eletrónico.