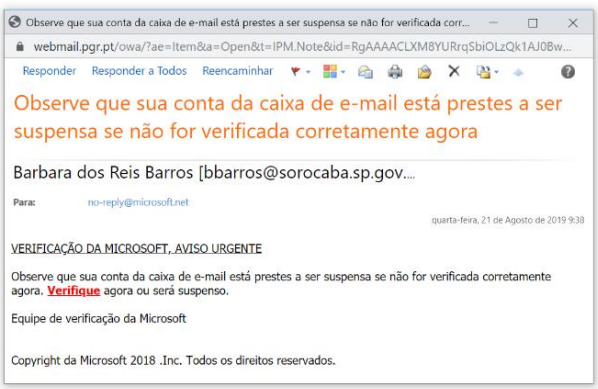
ALERTA CIBERCRIME

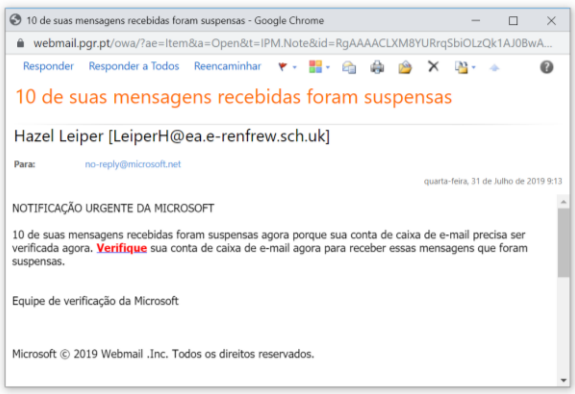
6 de setembro de 2019

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.

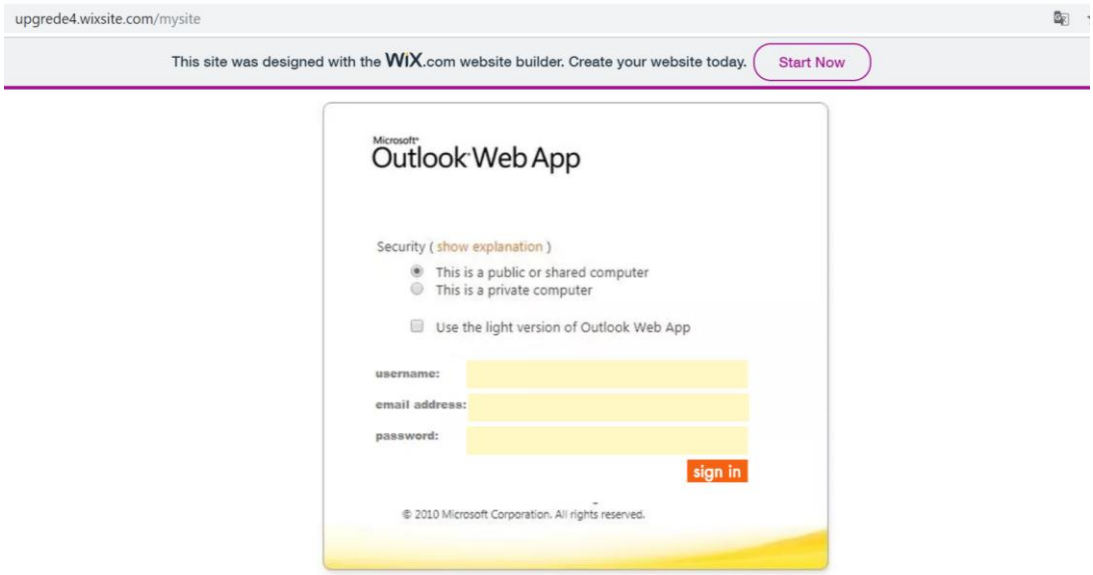
2. Trata-se de uma campanha consistente e continuada, a qual faz uso de contas de correio eletrónico legítimas, de entidades legítimas (elas próprias, vítimas de *phishing*). A este respeito foi já emitido um alerta (disponível aqui), a 2 de julho de 2019. Com efeito, nos diversos casos identificados nas últimas semanas, as mensagens criminosas foram sempre expedidas a partir de legítimas contas de correio eletrónico, de terceiros, sem o respetivo conhecimento, suspeitando-se que terá havido ilegítimo acesso às mesmas, para ulterior expedição das mensagens em causa.
Assim aconteceu no caso que deu origem ao alerta acima referido, de 2 de julho de 2019 (conta de *email* teresa.goncalves@abreu.pt), da mesma forma que assim aconteceu em casos identificados a 11 de julho de 2019 (conta de *email* vladimir.cacinovic@mps.hr), a 15 de julho de 2019 (conta de *email* mariagrazia.milillo@aas3.sanita.fvg.it), a 31 de julho de 2019 (conta de *email* LeiperH@ea.e-renfrew.sch.uk) e a 21 de agosto de 2019 (conta de *email* bbarros@sorocaba.sp.gov.br).





3. Todas estas mensagens foram expedidas com destino a uma suposta lista de distribuição NO-REPLY@MICROSOFT.NET, por uma suposta "*Equipe de verificação da Microsoft*" e, assumindo como "assunto" o de "*10 de suas mensagens recebidas foram suspensas*" ou, noutros casos, "*Observe que sua conta da caixa de e-mail está prestes a ser suspensa se não for verificada corretamente agora*".
Em caso de mensagem mais recente, de 2 de setembro de 2019 (conta de *email* udks@aim.gov.my) o "assunto" era "notificação Microsoft". Esta expressão é, aliás, referida em todas as mensagens que, genericamente, apelam para que o destinatário aceda a um *link* para que aí verifique "*sua conta de caixa de e-mail para receber mensagens que foram suspensas*".

4. As diversas mensagens indicam diferentes *links* (https://dgbnmdj.wixsite.com/mysite, https://hudtfeyd.wixsite.com/mysite, https://upgrede4.wixsite.com/mysite, ou ainda https://srsgddh.wixsite.com/mysite) que, quando acedidos, dirigem o utilizador para uma página *web.*
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, nenhuma destas mensagens fraudulentas foi remetida por qualquer serviço da 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 seu conteúdo é enganador. Não confere 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.