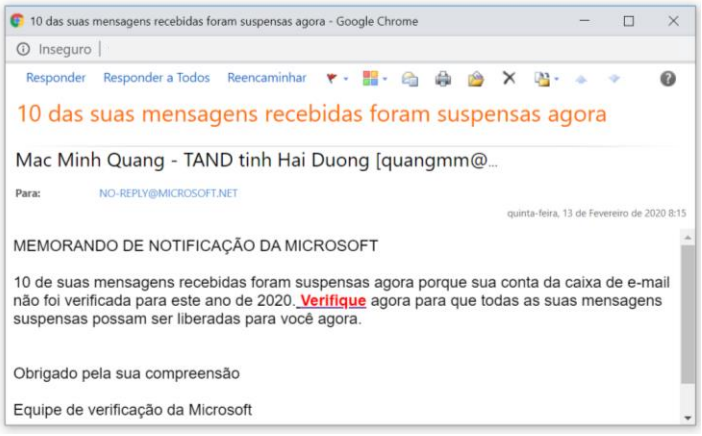
# ALERTA CIBERCRIME

**13 de fevereiro de 2020**

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

**1.** Está em curso mais 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.
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 foram já emitidos alertas (por exemplo, aqueles disponíveis aqui e aqui), durante o ano de 2019.

**2.** Vieram agora a ser identificados mais casos de mensagens criminosas.
Tal como já acontecera ao longo de 2019, as mensagens fraudulentas foram agora 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.

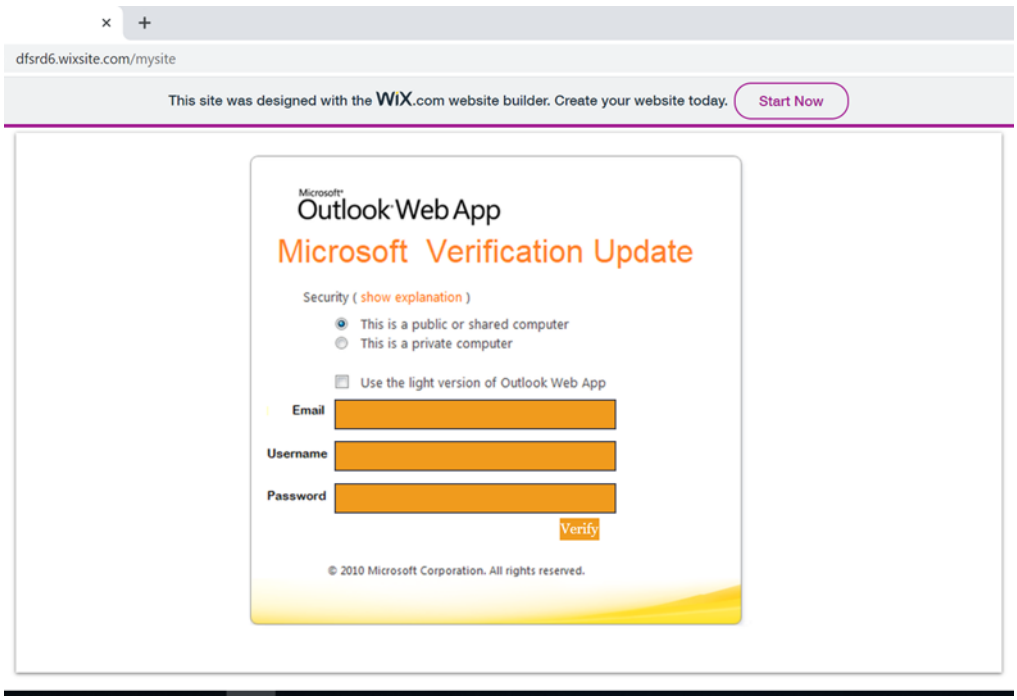



**3.** No caso agora identificado pelo Gabinete Cibercrime, a 13 de fevereiro de 2020, pelas 8 horas e 15 minutos, como já acontecera ao longo de 2019, as mensagens foram expedidas com destino a uma suposta lista de distribuição NO-REPLY@MICROSOFT.NET, por uma suposta "*Equipe de verificação da Microsoft*" e, assumindo como "assunto", o de "*10 de suas mensagens recebidas foram suspensas agora*".

Depois, no texto da mensagem, dizia-se que "*10 de suas mensagens recebidas foram suspensas agora porque sua conta da caixa de e-mail não foi verificada para este ano de 2020. Verifique agora para que todas as suas mensagens suspensas possam ser liberadas para você agora*." Embebido neste texto, indicava-se um *link* que o utilizador deveria acionar, para "verificar" as mensagens.

**4.** Além disso, embora a mensagem viesse assinada por uma suposta "*Equipe de verificação da Microsoft*", dela constava ser seu expedidor o endereço quangmm@toaan.gov.vn, pertencente a Mac Minh Quang. Veio a apurar-se ser servidor do Tribunal Popular da Província de Hai Duong, no Vietname. O domínio onde está alojado este endereço de correio eletrónico (https://www.toaan.gov.vn) pertence ao "*Tòa án nhân dân tối cao*", o Supremo Tribunal Popular da República Socialista do Vietname. Aliás, quanto à origem técnica da concreta mensagem identificada, verificou-se ter sido utilizado na expedição o endereço de IP 222.255.0.41, pertencente à "*VietNam Data Communication Company*", com sede em Hanói, no Vietname.

**5.** Tal como aconteceu nos casos identificados ao longo do segundo semestre de 2019, o *link* indicado nesta nova mensagem aponta para uma página *web* que, quando acedida, 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 endereço de correio eletrónico ("*Email*"), do nome do utilizador ("*Username*") e da senha de acesso à conta ("*Password*").




**6.** Porém, esta como as anteriores mensagens fraudulentas, não 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.

Por outro lado, esta nova página identificada 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.

**7.** Caso o utilizador use habitualmente a aplicação *Outlook Web App* para aceder a correio eletrónico de forma remota e, por acidente, introduzir nesta página fraudulenta as suas credenciais, deverá de imediato aceder à versão autêntica da mesma e nela proceder à alteração das suas credenciais de acesso.