ALERTA CIBERCRIME

14 de fevereiro de 2020

Falsos telefonemas da Microsoft

1. Está em curso uma campanha continuada de burlas por via de chamadas telefónicas fraudulentas em que, de forma astuciosa e enganosa, são abordados utilizadores da Internet em território nacional, alegadamente pelo "apoio técnico" da Microsoft. Trata-se de um método criminoso conhecido na gíria internacional como *Tech Support Scam*.

2. Nesta atividade criminosa, os "atacantes" contactam por telefone alvos selecionados, fazendo-se passar por uma suposta "equipa de assistência técnica da Microsoft". No contacto, a vítima é informada de que existe um problema técnico com o seu computador (normalmente um vírus) para o qual o "atacante" tem resolução.
Nalguns casos, a vítima é "conduzida" a instalar *software* que lhe é remetido por correio eletrónico, o qual resolverá o suposto problema. O *software* em causa é de origem maliciosa e, entre as várias ações, poderá danificar, roubar dados, encriptar ou até mesmo inutilizar o sistema.
Noutros casos, é solicitada à vítima que aceda a uma página na Internet onde lhe são solicitados dados que permitem ao "atacante" aceder remotamente ao computador daquela.
Noutros ainda, o "atacante" diz que consegue resolveu o problema mediante um pequeno pagamento e pede à vitima os dados do respetivo cartão de crédito, os quais mais tarde vem a utilizar em seu proveito, noutros pagamentos.

3. Estas chamadas telefónicas, que não têm origem na Microsoft, são fraudulentas, traduzindo em geral a prática de crimes de burla. Não têm origem em Portugal – muitas delas têm origem em países como a Índia e ou a Nigéria, ou outros, com quem a cooperação judiciária é mais complexa ou demorada, e visam vítimas de todo o mundo. Em geral, os criminosos selecionam os contactos

telefónicos de forma aleatória, em fontes abertas, na Internet, na esperança de que o destinatário do telefonema seja utilizador de Windows, um produto Microsoft.

4. Normalmente, se a tentativa de burla não for bem sucedida, a ação criminosa não vai mais longe e fica por aí. Isto é, se a vítima não aceder aos intentos do "atacante" e evitar proceder da forma que aquele sugere, ou se a vítima manifestar que percebe estar a ser abordada por um criminoso, este não volta a telefonar e procura outras vítimas.

5. É pois recomendável que, tal como acontece nos casos de "*phishing*" por correio eletrónico, os utilizadores avaliem cautelosamente as comunicações que recebam, nunca fornecendo informações pessoais ou de cartões de crédito, e não instalando qualquer tipo de *software* que lhe seja indicado telefonicamente.