ALERTA CIBERCRIME

3 de novembro de 2021

Falsos telefonemas da Microsoft

1. Está em curso uma continuada campanha criminosa 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 aleatoriamente, 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: em geral, referem que o computador está infetado com um vírus, ou foi atacado por hackers. Depois, informam que têm resolução para o problema.

Foram identificados alguns casos em que a vítima foi "conduzida" a instalar *software* que lhe foi remetido por correio eletrónico (o qual seria adequado a resolver o suposto problema). Normalmente, este *software* é de origem maliciosa e pode danificar, roubar dados, encriptar ou até mesmo inutilizar o sistema.

Noutros casos detetados, foi sugerido à vítima que acedesse a uma página na Internet e aí introduzisse dados confidenciais, como os do seu cartão de crédito ou de acesso à sua conta de email.

Foram ainda identificadas situações em que o "atacante" pediu à vítima que partilhasse o seu ecrã e que, mantendo o ecrã partilhado, acedesse à sua conta de *homebanking*.

Noutros casos referenciados, o "atacante" afirmou conseguir resolveu o problema técnico mediante um pequeno pagamento, que a vítima podia pagar com o respetivo cartão de crédito (cujos dados então solicitou, ficando assim em posição de os vir a utilizar mais tarde, em seu proveito).

3. Estas chamadas telefónicas não têm origem em nenhum serviço ou departamento da Microsoft e são fraudulentas, traduzindo em geral a prática de crimes. 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 difícil 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 ou outro produto Microsoft.
Depois, ardilosamente, induzem as vítimas em erro, convencendo-as a fornecer-lhes os seus dados pessoais, de acesso a contas bancárias, ou de cartões de crédito.

4. Normalmente, se a tentativa 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. Este tipo de fraude tem vindo a sofrer um grande incremento, num contexto em que há muitas pessoas a trabalhar a partir de casa, usando serviços e sistemas informáticos aos quais acede remotamente – estando, portanto, mais dependentes das estruturas tecnológicas. Os criminosos exploram o desconhecimento, a incerteza e a dúvida das vítimas.

6. É, pois, recomendável que os utilizadores de sistemas informáticos avaliem cautelosamente as respostas que dão a comunicações telefónicas que recebam, nunca fornecendo informações pessoais ou de cartões de crédito, e não instalando qualquer tipo de *software* que lhes seja indicado telefonicamente por desconhecidos.