ALERTA CIBERCRIME

22 de junho de 2026

Falsos telefonemas da Paypal

1. Está em curso uma continuada campanha criminosa por via de chamadas telefónicas fraudulentas em que, de forma astuciosa e enganosa, as vítimas são abordadas alegadamente pelo "serviço de apoio" da *Paypal*. Trata-se de uma campanha levada a cabo por grupos estrangeiros de crime organizado pela qual, por meio de técnicas de engenharia social, os agentes criminosos procuram obter, de forma ilícita, acesso a contas *Paypal* para, a partir delas, serem feitos pagamentos em seu proveito.

2. Nesta atividade criminosa, a vítima é sempre abordada por telefone, em inglês. Quando atende, uma mensagem gravada refere que foi efetuada uma compra paga com a sua conta *Paypal*, sugerindo que, caso pretenda solicitar a anulação da mesma, prima uma tecla no seu telefone. Se a vítima o fizer, é direcionada para um suposto funcionário da *Paypal*, que lhe confirma que, pela respetiva conta, foi efetuada uma compra suspeita. Com frequência, a narrativa dos agentes criminosos refere compras de criptoativos para destinos na Rússia, ou na China. Também foram identificados casos em que o agente criminoso argumentou que o computador da vítima pode ter sido "invadido" por um *hacker*, que terá capturado as suas credenciais de acesso à conta *Paypal*.

3. Como se trata de um pagamento "inventado" pelo agente criminoso, claro que a vítima nega ter sido ela a efetuar aquela compra. Porém, esta abordagem provoca na vítima o receio de perder o valor em causa. O agente criminoso oferece-se então para ajudar a anular tal movimento: sugere mandar à vítima, por correio eletrónico, um *link* onde a mesma pode descarregar, para o seu computador, *software* que vai ajudá-la a solucionar a questão. Foram identificados diversos casos em que a vítima foi "conduzida" a instalar *software* comercialmente disponível que permite o acesso remoto a computadores (*TeamViewer*, *AnyDesk*, *UltraViewer*).

4. Após a instalação desse *software*, o agente criminoso acede remotamente ao computador da vítima, passando a monitorizar e controlar todas as instruções e todos os comandos inseridos no mesmo. Sugere então à vítima que aceda à respetiva conta *Paypal*.
Foram identificados casos em que o agente criminoso simplesmente se apoderou das credenciais de acesso a essa conta, mas também foram identificados casos em que, alegadamente para se proceder à reversão do suposto pagamento não autorizado, o agente criminoso convenceu a vítima a proceder, ela mesma, a pagamentos a terceiros.

5. Estas chamadas telefónicas não têm origem em nenhum serviço ou departamento da *Paypal* e são fraudulentas. Todo este procedimento dos agentes criminosos é uma encenação: os mesmos não têm qualquer função na *Paypal* e o suposto movimento "suspeito" não existiu nunca. Embora as chamadas pareçam provir de números telefónicos portugueses, têm sido identificado que as mesmas têm origem, entre outros, em países do sudoeste asiático. Este tipo de fraude não é especificamente direcionada para Portugal, antes visando vítimas em todo o mundo. Em geral, os criminosos selecionam os contactos telefónicos de forma aleatória, na esperança de que o destinatário do telefonema seja detentor de uma conta *Paypal*.

6. Normalmente, se a tentativa não for bem-sucedida – isto é, se a vítima se aperceber que está a ser alvo de uma fraude –, a ação criminosa não vai mais longe e fica por aí. Isto é, se a vítima não aceder aos intentos do agente criminoso e evitar proceder da forma que aquele sugere, ou se a vítima manifestar que percebe estar a ser abordada por um criminoso, este desliga o telefonema e procura outras vítimas.

6. É recomendável que se avaliem cautelosamente as respostas a comunicações telefónicas desta natureza, nunca se fornecendo informações pessoais ou de cartões de crédito, e não instalando qualquer tipo de *software* indicado telefonicamente por desconhecidos.