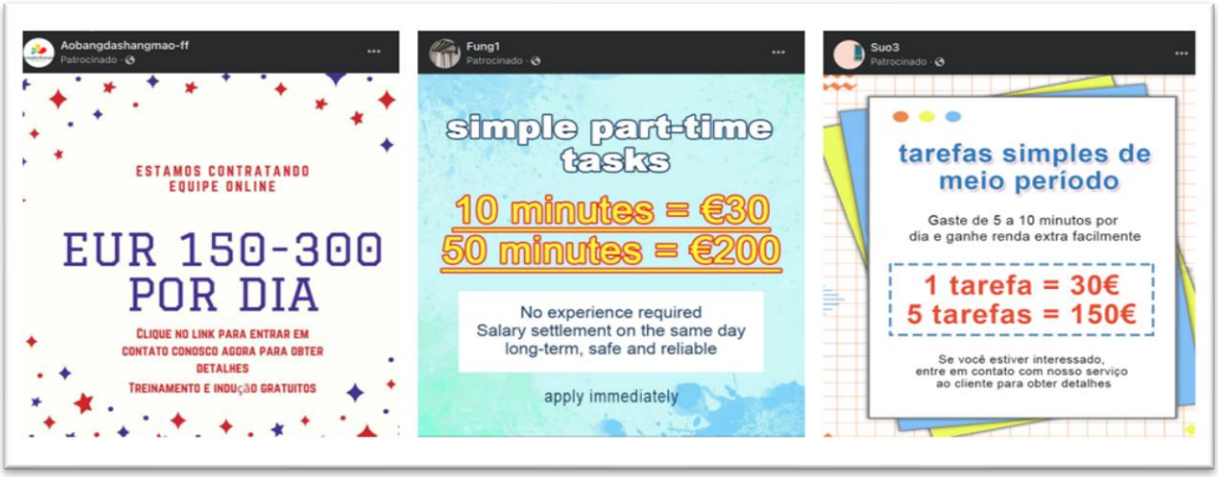
ALERTA CIBERCRIME

27 de janeiro de 2023

Burlas em "Trabalho Online"

1. Estão em curso campanhas de burlas por via das redes de comunicações, que passam pela simulação da contratação de pessoas para prestarem serviços *online*, as quais têm como propósito enganar os candidatos a trabalhadores, para deles vir a obter benefícios patrimoniais.

2. Os agentes criminosos procuram as suas vítimas por meio da difusão de anúncios na Internet, designadamente em redes sociais. Em tais anúncios informam que estão a recrutar pessoas para postos de trabalho *online*. Solicitam às vítimas formas de contacto direto.



3. Identificaram-se casos em que, apesar de não terem respondido a anúncios, as vítimas foram abordadas por via das formas de contacto que as mesmas disponibilizaram em portais de emprego ou em plataformas ou redes profissionais (como o LinkedIn, por exemplo).

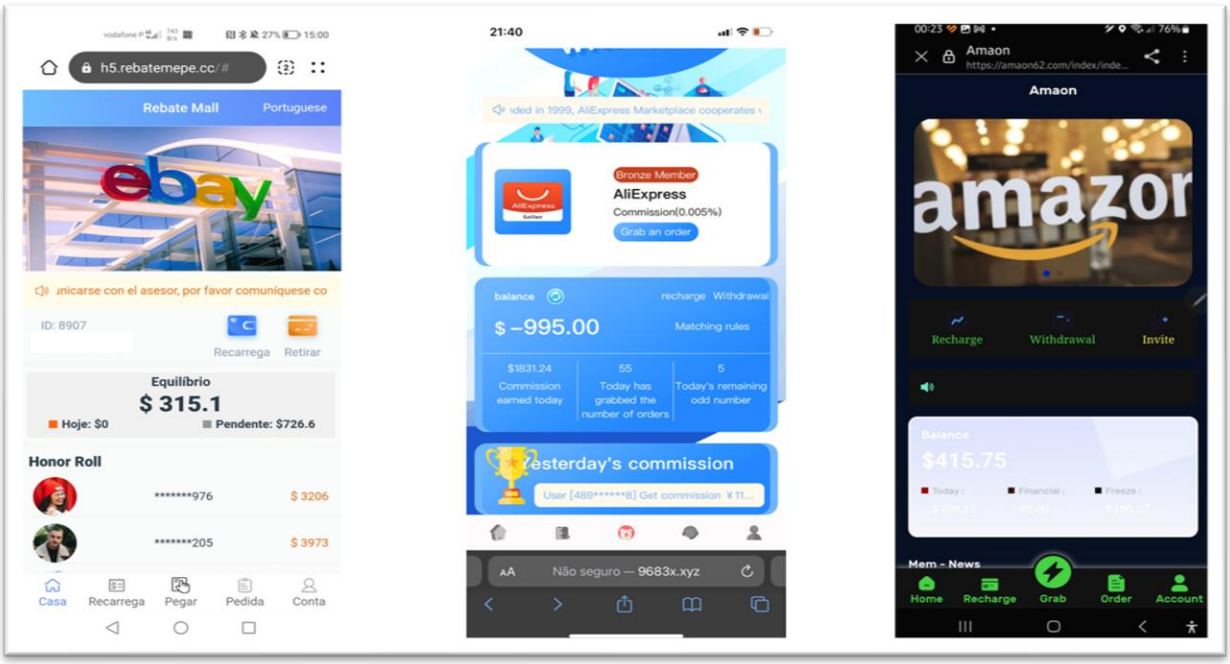
4. De acordo com este método criminoso as vítimas são sempre abordadas de forma individual e personalizada, por via de mensagens de WhatsApp ou, por vezes, de Telegram. Nesta abordagem, o criminoso informa a vítima de que foi selecionada para um posto de trabalho *online*, que poderá cumprir a partir de casa, o qual lhe renderá quantias de algumas centenas de euros por dia. Para esse efeito terá apenas que executar pequenas tarefas *online*. Também por via de mensagens de WhatsApp ou de Telegram (e nunca por abordagem pessoal ou chamada de voz ou vídeo), os agentes criminosos dão instruções para a execução dessas tarefas.

5. A narrativa e encenação utilizada pelos diversos grupos criminosos é variada. Em muitos dos casos referenciados foi pedido às vítimas que ficticiamente fizessem compras *online*, sem que as compras se concretizassem efetivamente. Esta simulação teria apenas, segundo os criminosos, o propósito de

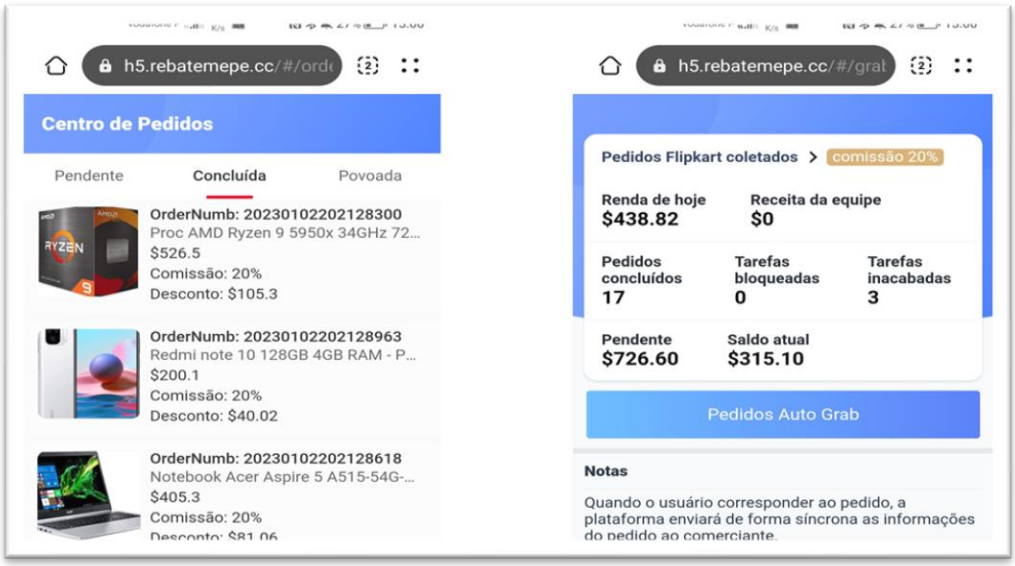
aumentar a visibilidade de certos comerciantes – que estavam dispostos a pagar por isso. Embora esta atividade suponha que as vítimas gastem dinheiro, é-lhes sempre prometido que todo ele lhes será devolvido, acrescido de uma comissão.
Em todas estas situações os criminosos facultam às vítimas o acesso a uma carteira de criptomoedas, a qual devem usar na sua atividade. Invariavelmente tais carteiras estão criadas em plataformas desconhecidas – controladas pelos agentes criminosos. Apesar de fraudulentas, tais plataformas procuram imitar, aos olhos do utilizador comum, conhecidas plataformas de comércio eletrónico.

6. Neste esquema fraudulento, é também solicitado à vítima que abra uma outra conta, na plataforma Binance, por via da qual esta mesma vítima deve comprar, com dinheiro seu, criptomoedas que depois transferirá para a sua conta na plataforma fraudulenta. Ou seja, além de terem que gastar valores seus que supostamente depois recuperam, as vítimas têm ainda que fazer circular tais valores entre duas contas: uma delas aberta na plataforma criminosa e a outra na plataforma Binance.

7. Após ser "convencida" a trabalhar, a vítima começa a cumprir as tarefas que lhe são determinadas, gastando dinheiro *online*, como lhe é dito para fazer. Após o cumprimento das tarefas, nos primeiros dias do processo, aparentemente são-lhe efetivamente devolvidas as quantias gastas, acrescidas de comissões, as quais são depositadas na conta da plataforma fraudulenta, para que possa continuar a gastar esses valores.



Porém, na verdade, esta informação produzida pela plataforma fraudulenta não é verdadeira. As despesas efetuadas pela vítima não são reais: a sua execução é mero resultado do *software* incorporado naquela plataforma, que cria a ilusão de que se efetuam compras, transferências e ganhos, as quais, na realidade, são totalmente inexistentes. A plataforma simula todas estas operações, da mesma forma que simula os valores supostamente ganhos como comissões.



Portanto, os valores que a vítima vê crescer na sua conta são totalmente fictícios. O único movimento verdadeiro é a transferência que a vítima faz, de criptomoedas, da sua conta na plataforma Binance para a plataforma fraudulenta, controlada pelos agentes criminosos.

8. Nos casos identificados, depois de alguns dias de atividade em que sempre se geraram comissões (fictícias), os agentes criminosos pedem às vítimas que estas executem tarefas (gastos de valores) em montantes superiores aos que dispõem na conta na plataforma fraudulenta. Tendo confiança de que tais valores lhes serão devolvidos, gerando comissões maiores, muitas vítimas compram mais criptomoedas na plataforma Binance e transferem as mesmas para a conta na plataforma fraudulenta. Nalguns casos, tais valores adicionais têm sido de vários milhares de euros.
A partir desse momento, em que as vítimas aceitam transferir quantias adicionais para a sua conta na plataforma criminosa, os agentes criminosos manipulam o sistema fraudulento para que este lhes exija cada vez mais quantias. Se as vítimas desconfiam ou receiam, ou pura e simplesmente não têm dinheiro para comprar mais criptomoedas, e tentam reaver aquilo que transferiram, os agentes criminosos usam as mais variadas técnicas dilatórias para não devolver aqueles valores (erros técnicos, necessidade de pagamento de taxas legais ou imposição de comissões adicionais). Em muitos casos, perante a promessa de devolução mediante pagamento de taxas, as vítimas ainda transferem mais valores.
Porém, os mesmo não são nunca devolvidos.

9. Quando finalmente a vítima se apercebe de que todo o esquema é fraudulento e com isso confronta os representantes da plataforma, estes cancelam-lhe a conta, ficando assim a vítima impedida de aceder à mesma. Os agentes criminosos deixam de estar contactáveis por WhatsApp ou Telegram. Nalguns casos, desativam a própria plataforma, que assim deixa de estar disponível *online* e verdadeiramente desaparece.

10. Existem múltiplas plataformas fraudulentas desta natureza, que surgem e desaparecem segundo a conveniência dos agentes criminosos. Quando fazem desaparecer uma delas, de imediato, os seus donos abrem uma outra, do mesmo teor, noutra localização na Internet.
Normalmente, estas plataformas estão alojadas em servidores da chamada *cloud*. Assim, como exemplo, foram identificadas páginas deste teor no domínio www.amaon62.com, registado no fornecedor de serviços Internet "*Domains by Proxy, LLC*" (https://www.domainsbyproxy.com/), baseado no Arizona, Estados Unidos da América, o qual oferece aos seus clientes alojamento de domínios *com privacidade*, isto é, mantendo confidencial toda a informação respeitante aos proprietários dos domínios.

11. Este método criminoso tem atingido muitas vítimas em Portugal, incluindo jovens no início de percurso profissional e desempregados que procuram trabalho. Este tipo de vítimas são atraídas por promessas de alta rentabilidade com pequenos investimentos e nenhum risco para o capital aplicado. Normalmente, não verificam que é inexistente a informação na plataforma sobre quem é o seu proprietário e quais os respetivos contactos (por exemplo, nunca é indicado um escritório físico ou números de telefone).
As vítimas também não se apercebem de que, embora as plataformas fraudulentas procurem imitar outras legítimas plataformas de comércio eletrónico, os seus nomes de domínio não correspondem àquelas, designadamente incluindo caracteres diferentes ou adicionais (como o exemplo já acima referido, do domínio www.amaon62.com, ou ainda o domínio www.aliexpress234.com também relacionado com práticas fraudulentas deste teor).
Nalguns casos, estas plataformas estão também associadas a "*esquemas de pirâmide*", nos quais as vítimas são solicitadas, elas mesmas, para fazer parte do processo criminoso.