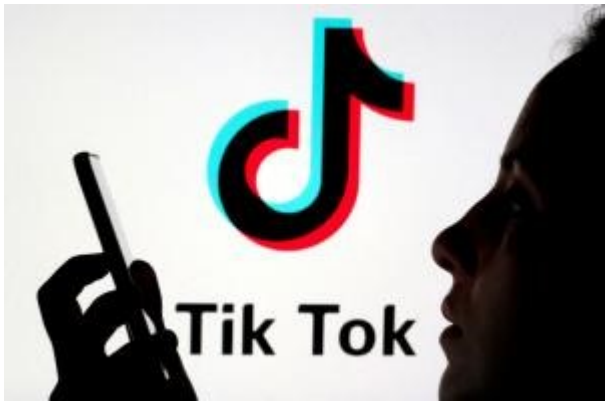
Não, o TikTok não está a recrutar trabalhadores. É uma burla

publico.pt/2024/04/13/tecnologia/noticia/nao-tiktok-nao-recrutar-trabalhadores-burla-2086824



Prova dos Factos

Burlões prometem rendimentos diários até 800 euros, pedindo às vítimas para aderir a grupos no WhatsApp. Não entre nestes grupos e não clique nos *links* que ali são partilhados.

Há uma nova burla: nos últimos dias, várias pessoas têm recebido chamadas ou mensagens de alguém que se apresenta como um funcionário do TikTok que está supostamente à procura de 100 novos trabalhadores *online*. São prometidos rendimentos diários entre 50 a 800 euros e, para tal, é dito que basta juntar-se a um grupo do WhatsApp. **Por muito tentador que seja, não o faça.**

“Devemos desconfiar de ofertas fantásticas à partida, da mesma forma que desconfiaríamos se alguém nos viesse oferecer um Ferrari na rua, no mundo real”, aconselha Bruno Castro, CEO da Visionware, empresa especializada em segurança da informação.

E sim, até é verdade que o TikTok – o verdadeiro – chegou a dada altura a oferecer dinheiro a utilizadores que convidassem amigos para utilizar a aplicação. **Mas o que está a acontecer agora é uma burla**, executada por criminosos que não têm qualquer relação real com o TikTok.

A má notícia é que é “muito difícil evitar” receber estas chamadas ou mensagens fraudulentas, mesmo que se tenha cuidado nos sítios onde se deixam dados pessoais. Grupos de *hackers* atacam empresas e roubam os contactos e registos destas, ou compram grandes bases de dados à venda na *dark web*. A partir daí, tentam contactar as pessoas que delas constam.

O segredo para chegar às vítimas, explica Bruno Castro, está na grande escala do ataque. Se uma base de dados tiver 100.000 pessoas e apenas 1% cair no engodo, são mil lesados: “muitas vítimas, mesmo que a percentagem seja baixa”, diz o especialista.

Ainda que possam não parecer – pela escrita estranha das mensagens ou pela voz robótica que se ouve nas chamadas no caso desta nova burla – estas são “acções mecanizadas muito profissionais”, que se dividem essencialmente em três fases.

A primeira: criar uma oferta altamente atraente (ou uma preocupação que possa chegar a um grande número de indivíduos). É o exemplo do tal trabalho *online* muito bem pago que é referido nesta burla, mas que não existe.

Se se passar desta primeira fase – no caso específico desta burla, se se entrar no *link* de um grupo onde supostamente estarão os outros candidatos à mesma vaga – vai haver uma tentativa de criar confiança e credibilidade através de uma comunicação constante. Essa é a segunda fase – enviam-se vídeos e perfis de TikTok, pede-se para colocar um *like* e a vítima fica numa zona intermédia pré-fraude.

Por fim, chega a fraude propriamente dita, o golpe. Há “mais de 30 mil formas” de enganar quem chega até esta terceira fase. Neste caso, em que a mensagem inicial promete um trabalho no TikTok, o CEO da Visionware descreve duas situações possíveis. Os burlões podem enviar um *link* que alegam ser do *site* de registo na empresa (mas não é, é um golpe de *phishing*, para recolher dados das vítimas), ou pedem para descarregar e instalar um *software* supostamente necessário para trabalhar ou receber pagamentos. Nesta fase, as vítimas cedem dados pessoais como o número de Cartão de Cidadão, Número de Identificação Fiscal, IBAN, número de cartão de crédito, entre outros, muitas vezes sem questionar os pedidos ou pensar no perigo da acção.

E é aí que o pior pode acontecer, como o desvio de dinheiro da sua conta.

Contactada pelo PÚBLICO, a Polícia de Segurança Pública confirmou que já recebeu várias queixas relativas a esta nova burla. Em comunicado, a PSP deixa algumas recomendações genéricas que também se aplicam a este caso:

- **Evite responder a mensagens de texto não solicitadas e bloqueie ou denuncie a pessoa que as envia.**
- **Desconfie de qualquer conselho de investimento que prometa lucros significativos e imediatos. Evite partilhar informações pessoais e financeiras com um contacto *online*.**
- **Desconfie de promessas irrealistas e bloqueie o contacto.**
- **Garanta sempre que está a utilizar um *site*/aplicação fidedigna.**