



INTIC

Instituto Nacional de Tecnologias de Informação e Comunicação



Autoridade Reguladora de TIC

RECOMENDAÇÕES PARA IDENTIFICAR PERFIS FALSOS

No Facebook e Instagram

AUTENTICIDADE DOS PERFIS	1	Verifique sempre a autenticidade dos Perfis de altas figuras do Estado. Esses perfis são normalmente verificados, exibindo uma marca de verificação azul junto do nome ou cinza para empresas.
FOTO DE PERFIL	2	Foto de perfil única, genérica ou retirada da internet;
INFORMAÇÃO PESSOAL	3	Poucas ou nenhuma informação pessoal (cidade, trabalho, escola, etc.);
DATA DE CRIAÇÃO	4	Conta criada recentemente, sem histórico de publicações antigas;
PÚBLICO DESPROPORCIONAL	5	Muitos amigos em pouco tempo e de países aleatórios ou tem muito poucos amigos (menos de 50) com muito tempo de existencia.
PUBLICAÇÕES	6	Publicações repetitivas ou copiadas de outros perfis;
MÚLTIPLOS PERFIS	7	Nome ou fotos aparecem em múltiplos perfis ao pesquisar na internet;
INCONSISTÊNCIA	8	Inconsistência entre fotos, publicações e comentários de amigos.
PEDIDOS	9	ESTE É O SINAL DE ALERTA MÁXIMO. Mensagens imediatas pedindo informações pessoais, links ou dinheiro;
ACTIVIDADE E CONTEÚDO	10	A linha do tempo está quase vazia ou tem longos períodos de inactividade e quando activa perfil só partilha links, memes ou vídeos de outras páginas, mas quase não tem publicações originais ou pessoais.



NORMALMENTE OS PERFIS FALSOS NO FACEBOOK OSTENTAM CARACTERÍSTICAS MENCIONADAS NOS PONTOS ACIMA REFERIDOS.

SE ESTAS CARACTERÍSTICAS FOREM NOTADAS, OU CASO HAJA DESCONFIANÇA EVITE INTERAÇÕES E IMEDIATAMENTE DENUNCIE A CONTA DIRECTAMENTE NO FACEBOOK OU PODE SOLICITAR O APOIO DO CSIRT NACIONAL.

O QUE FAZER SE SUSPEITAR?

1

Não aceite a solicitação de amizade. Para evitar que as pessoas falsas tenham acesso a uma grande quantidade de informações suas, como seus post, fotos, família, hábitos e opiniões.

2

Não clique em links que a pessoa enviar. Links maliciosos são uma das ferramentas mais comuns dos criminosos online. Clicar em um link enviado por um perfil falso pode levar a várias consequências graves: Phishing, Scam e malwares.

3

Bloqueie e Denuncie imediatamente tais perfis às autoridades competentes e à própria plataforma de rede social Facebook ou Instagram através de "Denunciar perfil". Ajude no combate a fraudes.

4

Avise amigos em comum sobre a suspeita. Proteja seus amigos: Muitas pessoas, especialmente idosos ou menos familiarizados com tecnologia, podem não reconhecer os sinais de um perfil falso e acabar aceitando a solicitação ou caindo em um golpe. Seu aviso pode preveni-los.

5

Confirme as postagens em canais oficiais, comunicados nos websites institucionais ou em outros meios de comunicação social. Para que não caia em desinformação.



DENUNCIE A CONTA DIRECTAMENTE NO FACEBOOK, INSTAGRAM OU PODE SOLICITAR O APOIO DO CSIRT NACIONAL.

CONTAMOS COM A COLABORAÇÃO DE TODOS PARA A SEGURANÇA DIGITAL, PRESERVAR A VERDADE, E A CONFIANÇA NAS INSTITUIÇÕES DEMOCRÁTICAS.

reportar@csirt.mz