ALERTA CIBERCRIME

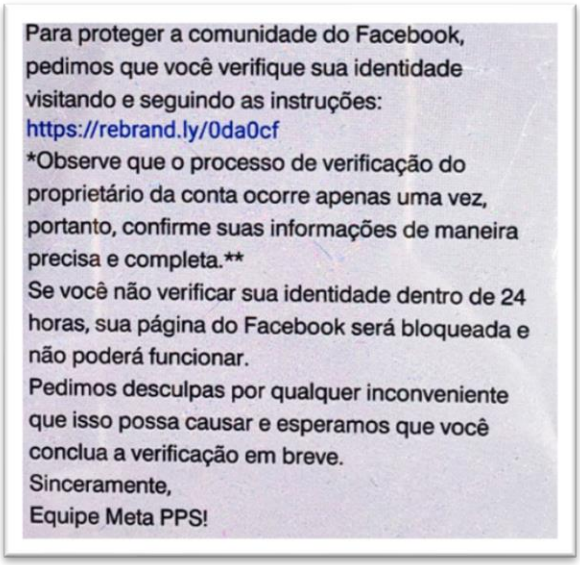
18 de setembro de 2023

"*Furto*" de contas

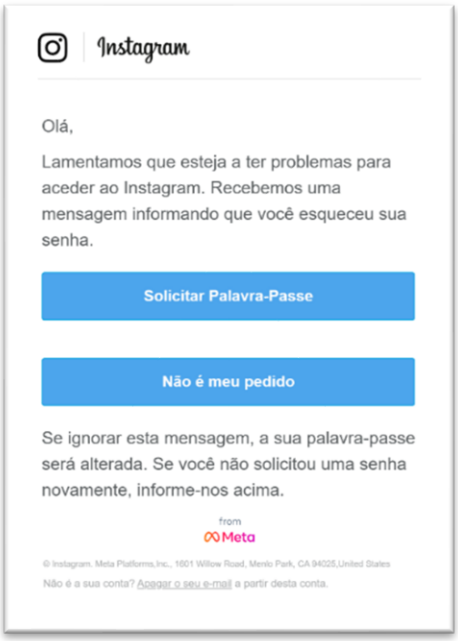
(apropriação de credenciais de acesso)

1. Tem sido recentemente noticiado ao Ministério Público um grande número de casos de **apropriação indevida de credenciais de acesso a contas, sobretudo de redes sociais** (em particular Instagram e Facebook). Isto é, de situações em que os agentes criminosos logram obter os códigos (*passwords*) de acesso a uma determinada conta, que depois alteram, assim impedindo o seu legítimo *dono* de a utilizar.

2. Normalmente, os agentes criminosos começam o processo identificando, na Internet, contas que não lhes pertencem, mas que lhes podem interessar. Fingindo serem os legítimos titulares da conta em causa, solicitam à plataforma que lhes faculte uma nova *password*, alegando que a esqueceram. Neste tipo de situações, as diversas plataformas costumam enviar códigos de autenticação para o telemóvel associado à conta, pertencente ao seu *dono*.


Para proteger a comunidade do Facebook, pedimos que você verifique sua identidade visitando e seguindo as instruções:
https://rebrand.ly/0da0cf
*Observe que o processo de verificação do proprietário da conta ocorre apenas uma vez, portanto, confirme suas informações de maneira precisa e completa.**
Se você não verificar sua identidade dentro de 24 horas, sua página do Facebook será bloqueada e não poderá funcionar.
Pedimos desculpas por qualquer inconveniente que isso possa causar e esperamos que você conclua a verificação em breve.
Sinceramente,
Equipe Meta PPS!

3. Para contornar este mecanismo, em paralelo, os agentes criminosos remetem ao *dono* da conta uma mensagem de correio eletrónico, ou WhatsApp, que simula ter origem no *serviço de apoio*, ou no *serviço de segurança* do Facebook ou do Instagram – também ocorre com outras plataformas, mas estas têm sido as mais visadas. Esta mensagem fraudulenta refere que está em curso uma tentativa de acesso à conta da vítima, por terceiros desconhecidos. Solicita, por isso, que sejam confirmados todos os dados e códigos de acesso à conta. Pede que tais dados sejam inseridos numa página (*link*) que indica. Tal *link*, se acedido, parece abrir uma legítima página da rede social em causa. Porém, assim não é: trata-se sempre de uma página falsa, gerida pelos agentes criminosos.


Instagram

Olá,

Lamentamos que esteja a ter problemas para aceder ao Instagram. Recebemos uma mensagem informando que você esqueceu sua senha.

Solicitar Palavra-Passe

Não é meu pedido

Se ignorar esta mensagem, a sua palavra-passe será alterada. Se você não solicitou uma senha novamente, informe-nos acima.

from Meta

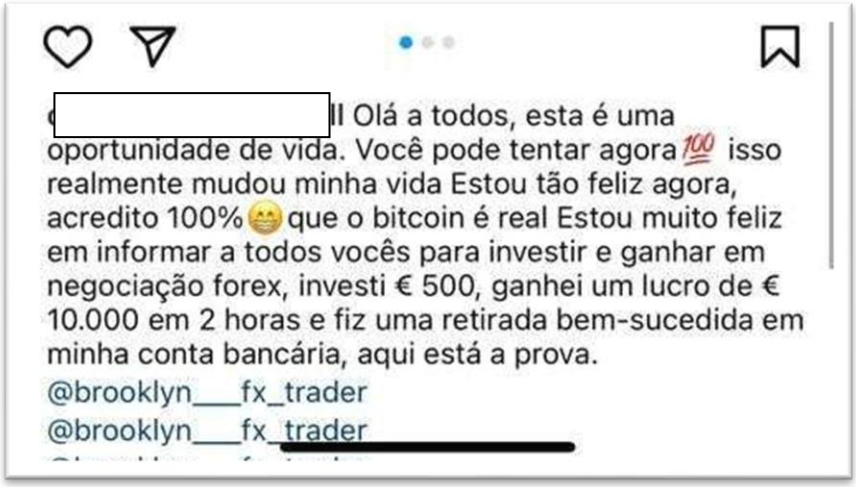
Não é a sua conta? Apagar o seu e-mail a partir desta conta.

Em regra, é solicitado ao *dono* da conta que copie e cole, em resposta à mensagem que recebeu, um código que lhe foi remetido, pela plataforma, para o seu telemóvel – o tal código, acima referido.
Se a vítima responder, facultando as suas credencias e, sobretudo, enviando o código de segurança que recebeu no telemóvel, os agentes criminosos ficam habilitados a gerar uma nova *password* de acesso à conta e a aceder à mesma.

4. Em geral, logo de seguida, os agentes criminosos procedem à alteração da *password* e também do endereço de email associado à conta Facebook ou Instagram. Também alteram o número de telefone que é utilizado para recuperação da *password*. Desta forma, passam a poder aceder livremente à conta, controlando-a completamente, ao mesmo tempo que inviabilizam, de todo, o acesso pelo seu legítimo titular.

5. Na generalidade dos casos identificados, trata-se de uma atividade levada a cabo por grupos criminosos organizados, com o propósito de lucro. Os diferentes grupos criminosos fazem diferentes utilizações fraudulenta das contas "furtadas", quer no caso das redes sociais, quer noutros (em especial, contas de correio eletrónico).

6. Quanto às contas Facebook e Instagram, numa boa parte dos casos identificados, as contas são utilizadas para difusão de mensagens de publicidade a plataformas de investimentos em criptomoedas. Invariavelmente, são plataformas fraudulentas, que não se dedicam a gerir legitimamente investimentos naquele tipo de ativos, mas antes têm como finalidade exclusiva defraudar os seus clientes. Esta publicidade pretende explorar a credibilidade que o *dono* da conta aufere junto dos seus amigos ou seguidores no Instagram.



7. Em muitos outros casos, o *dono* da conta tem sido abordado pelos criminosos, que lhe pedem um resgate, para lhe serem devolvidas as credenciais de acesso à conta. São alvo muito frequente deste tipo de atuação os chamados *influencers* e outros produtores de conteúdos *online*, cuja atividade na Internet tem como objetivo a obtenção de rendimentos económicos.

O mesmo sucede com negócios de venda *online* (venda de roupa, acessórios de moda, artesanato ou muitos outros) que, não tendo lojas físicas, dependem de visibilidade na Internet.

Tem sido noticiado um grande número de casos de "furto" de credenciais de páginas deste tipo, os quais têm importantes consequências pecuniárias para os visados.

Algumas destas páginas e destes negócios têm ficado irremediavelmente prejudicados. É recomendável que os gestores de páginas ou plataformas desta natureza tenham particular atenção a mensagens que solicitam a "confirmação" de credenciais de acesso.

8. Além de obtenção ilícita de *passwords* de acesso a redes sociais, tem também sido recorrentemente noticiada ao Ministério Público o mesmo tipo de prática criminosa dirigida a contas de correio eletrónico, as quais são depois utilizadas para diversas atividades ilícitas.

9. Por via deste tipo de procedimento criminoso, os seus autores (aparentemente, com ligações à África Ocidental e à Rússia, mas ocasionalmente também a outras regiões) pretendem induzir as vítimas a facultar-lhes um modo de acesso às suas contas, para depois poderem ilegitimamente aceder às mesmas e fazer delas uma utilização abusiva, com intuito de obtenção de vantagens patrimoniais.

Este método explora a grande facilidade que existe de acesso às diversas contas e plataformas a partir dos mais diversos dispositivos. Por outro lado, explora o impulso, quase instintivo, de reação imediata a comunicações eletrónicas que incitem à adoção de medidas de segurança.

10. Mensagens como as que acima se descreveram, solicitando o fornecimento de dados de autenticação de contas, devem ser cautelosamente avaliadas. Os *links* que indicam devem ser cuidadosamente verificados. Caso as mensagens se afigurem duvidosas, não deve responder-se às mesmas, devendo antes tais mensagens ser comunicadas ao Ministério Público ou aos órgãos de polícia criminal.