Manual de configuração de segurança nos aplicativos Whatsapp e Telegram

Diante dos noticiados vazamentos de informações privadas de autoridades, preparamos um tutorial para melhorar a segurança das informações das autoridades da Justiça Federal da 1ª Região.

O tutorial é focado nos dois principais mensageiros: Whatsapp e Telegam. As imagens são de um celular Android, mas as configurações são análogas em celulares Apple (iOS).

De maneira geral, os passos são:

1- Identificar quais sessões do aplicativo estão ativas, e analisar se existe alguma atividade suspeita.
2- Habilitar as opções de autenticação de 2 fatores (senha para acessar o app de qualquer lugar)
3- Habilitar as opções de privacidade do aplicativo (senha para acessar o app no celular).

Faremos, ainda, uma breve discussão sobre como os atacantes podem ter tido acesso às conversas das autoridades.

Identificando sessões ativas dos aplicativos

Ambos os aplicativos permitem que mais de uma sessão estejam ativas ao mesmo tempo: é o caso do Whatsapp Web, e do Telegram web.

Se forem identificadas sessões ativas que desconheça a procedência (será explicado e exemplificado a seguir), o número pode ter sido comprometido e recomendamos que entre em contato com a SESEI e/ou órgãos de segurança. Entretanto é importante ressaltar que não identificar sessões estranhas não significa que o aplicativo não foi comprometido, pois alguém mal intencionado pode ter apagado seus rastros.

Após seguir as etapas aqui apresentadas o aparelho estará seguro contra ataques do tipo 'clonagem de chip', pois além do código SMS que o aplicativo envia para o aparelho, será necessário ainda informar a senha definida pelo usuário para que o aplicativo seja vinculado ao número e funcione corretamente. Ressaltamos que a segurança se dá a partir da configuração, e não se pode garantir que não houve comprometimentos passados.

Whatsapp

O whatsapp permite que o app seja utilizado em apenas 1 aparelho simultaneamente. Entretanto o usuário pode se conectar em vários navegadores pelo 'whatsapp web'. A seguir mostramos como identificar quais sessões do whatsapp web estão ativas, e como desativá-las.

1) Abra o whatsapp e clique no Menu, na tela inicial (ícone de 3 pontinhos)

Figura 1

2) Clique na opção "Whatsapp Web". Caso exista alguma sessão ativa no aplicativo, ela será listada conforme Figura 3. Caso não exista outra sessão ativa, o aplicativo irá abrir a câmera para ler um QR code.

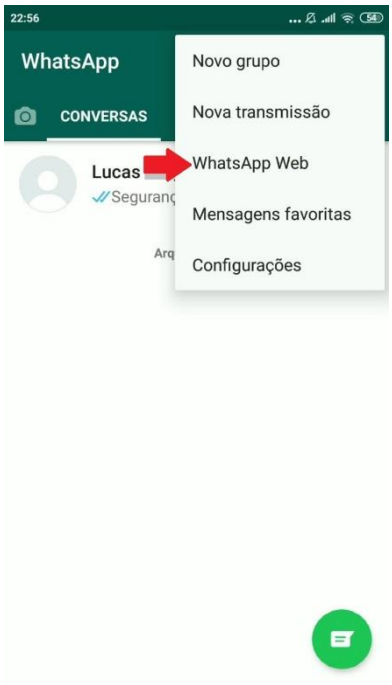


Figura 2

3) A Figura 3 mostra um exemplo de aplicativo com sessões ativas. Verifique se reconhece as sessões que aparecerão no seu aplicativo. As sessões são de navegadores da web onde o aparelho fez o uso do 'whatsapp web' e podem ser antigas. Ainda que não identifique irregularidades, recomendamos que clique em "Sair de todas as sessões?" para que apenas a sessão do seu aparelho permaneça ativa.

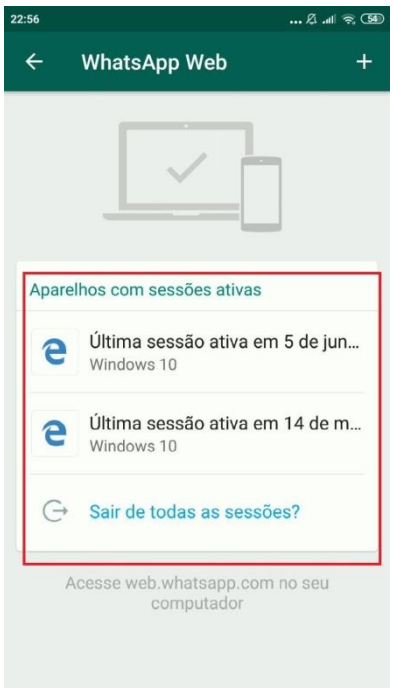


Figura 3

Telegram

Diferentemente do Whatsapp, o Telegram permite que a mesma conta esteja ativa em vários aparelhos celulares diferentes, além de também possuir a versão 'web'. A seguir é mostrado um passo a passo de como identificar quais sessões da conta estão ativas.

1) Abra o mensageiro Telegram e clique no menu, as 3 linhas horizontais paralelas no canto superior, conforme Figura 4.

Figura 4

2) No menu que se abrirá, clique em "Configurações".

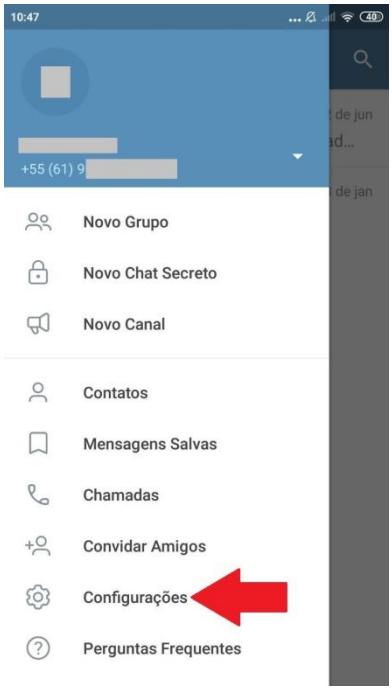


Figura 5

3) Clique agora na opção “Privacidade e Segurança”.

Figura 6

4) Para verificar quais sessões do aplicativo estão ativas, clique em “Sessões Ativas”.

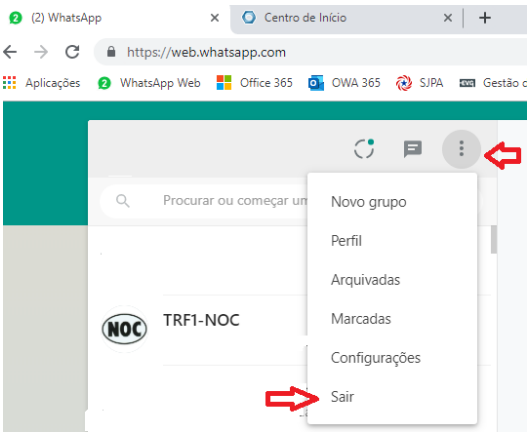
Figura 7

5) Analogamente ao Whatsapp, aqui são mostradas as sessões do aplicativo que estão ativas em outros dispositivos. Recomendamos que se analise essa lista para identificar se existem sessões ativas em dispositivos não reconhecidos, principalmente aparelhos celulares estranhos ou sessões em navegadores não reconhecidos. Caso não identifique nada de anormal, ainda assim recomendamos que clique em "Terminar todas as outras sessões", para que apenas a sessão do seu aparelho permaneça ativa.

Figura 8

Recomenda-se, como medida preventiva, sair de todas as seções ativas, eliminando a possibilidade de utilização dos acessos WEB em outros dispositivos na ausência do titular.

Recomenda-se ainda, quando da utilização das versões WEB dos aplicativos em microcomputadores alheios (hotéis, aeroportos...), observar a necessidade de sair do aplicativo ao final de sua utilização, caso contrário o próximo utilizador do navegador terá acesso integral às conversas, podendo enviar mensagens em nome do titular.



Autenticação de 2 fatores

Essa é a configuração que efetivamente vai prover segurança ao aplicativo, impedindo que tenham acesso aos seus dados sem que se possua uma senha que o próprio usuário definiu.

Whatsapp

Abra o Menu, clique em “Configurações”, depois em “Conta” e depois em “Confirmação em duas etapas”. Ative essa opção, siga os passos até o fim e escolha uma senha de 6 dígitos que não seja de fácil identificação, mas que você lembre com facilidade.

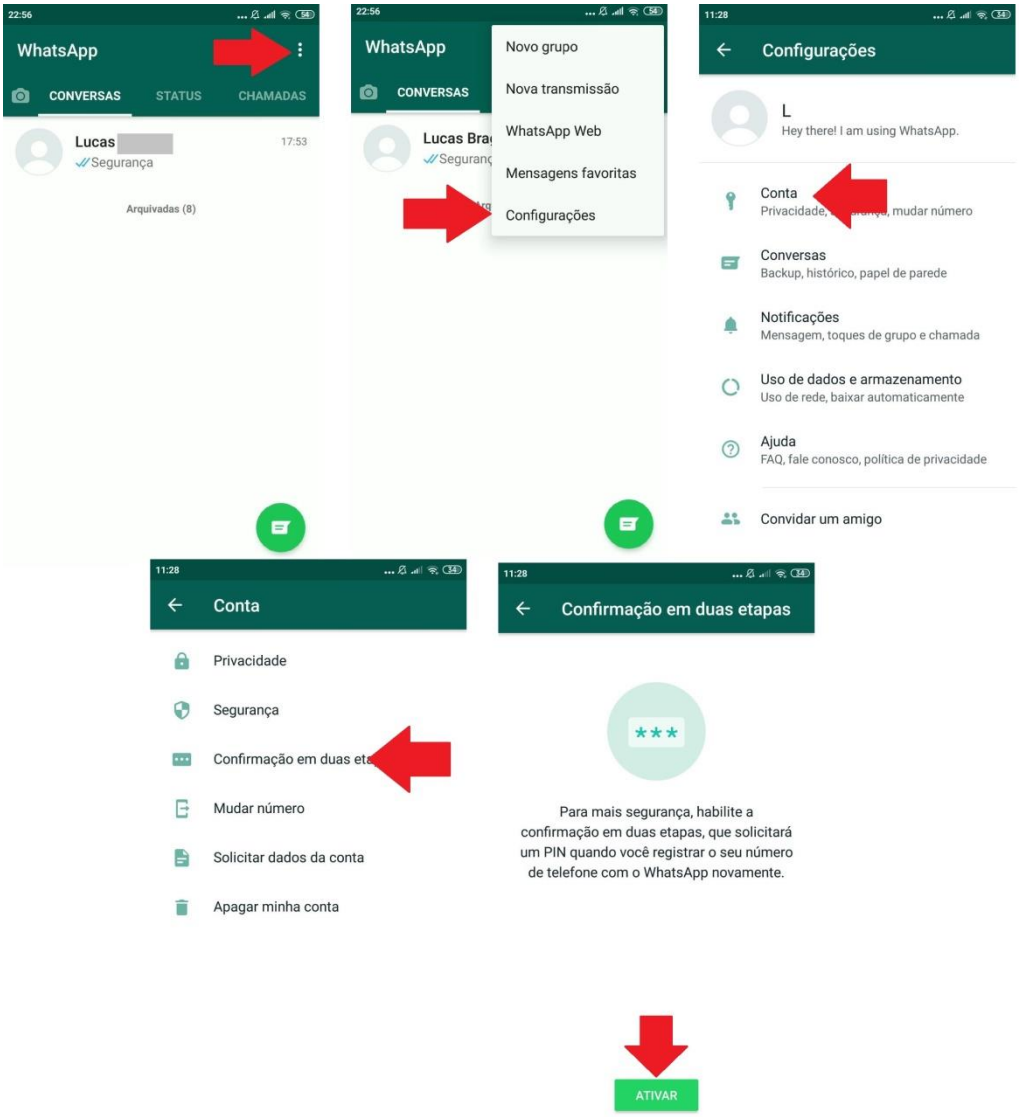


Figura 9

Telegram

Abra o Menu, clique em “Configurações”, depois “Privacidade e Segurança” e em seguida em “Verificação em Duas Etapas”. Clique em “Configurar senha adicional” e siga as instruções do App. Utiliza uma senha que não seja fácil de fácil identificação, mas que você possa lembrar com facilidade.

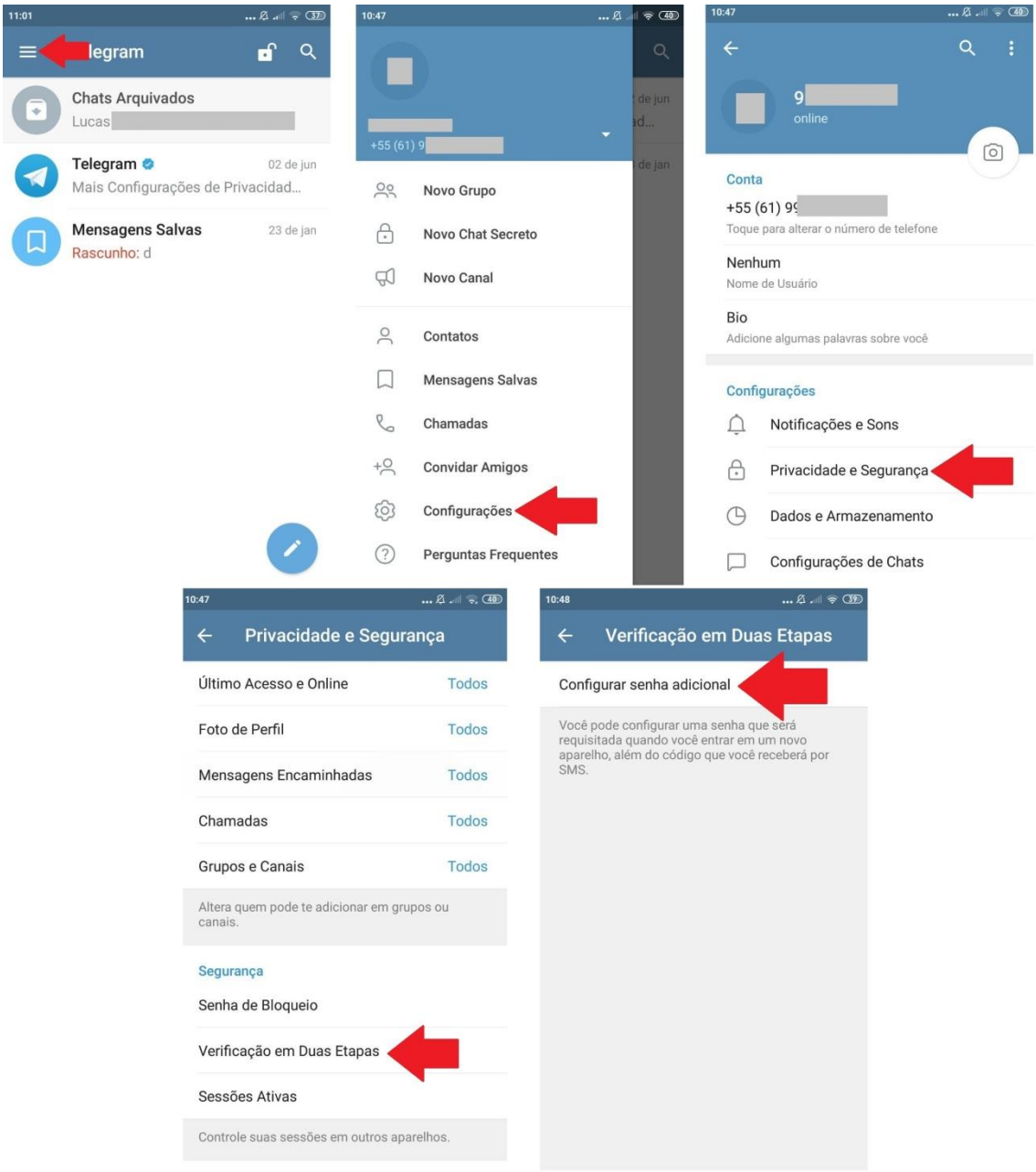


Figura 10

Senha de privacidade no aplicativo

O Telegram permite a definição de uma senha que é solicitada ao abrir o aplicativo no celular. Essa senha não está relacionada a ataques ou tentativas de invasão a distância, mas protege as mensagens e informações nos casos em que alguém tenha posse do seu aparelho. Para configurar, siga as instruções da Figura 11. O Whatsapp não possui essa opção nativamente.

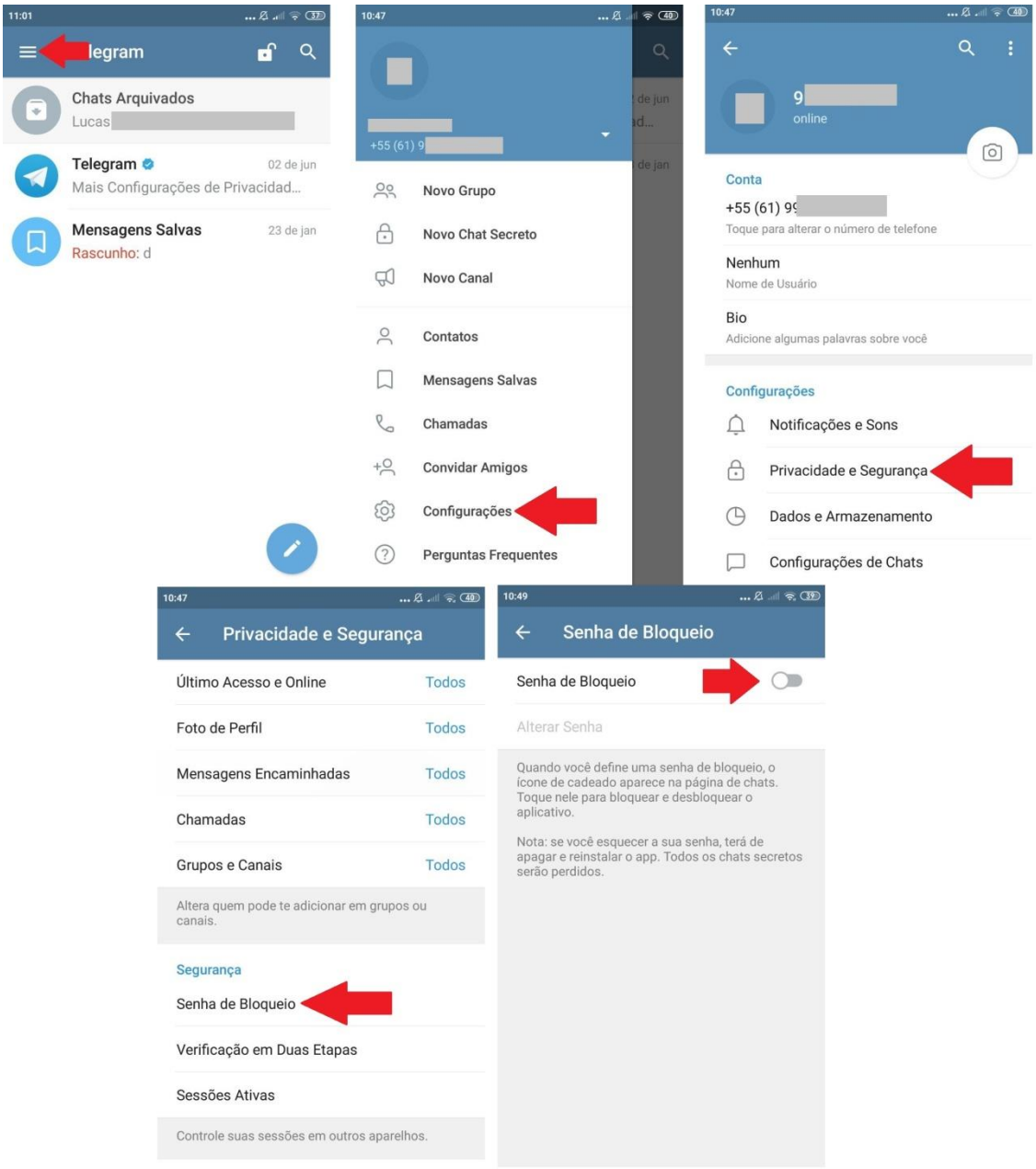


Figura 11

Comentários sobre os ataques às autoridades

Os recentes ataques ainda estão sob investigação, mas a hipótese mais provável é que ele tenha se baseado em uma clonagem do número de telefone das vítimas. Tal clonagem pode ser feita por alguém com privilégios dentro das operadoras telefônicas ou alguém se passando pela vítima e conseguindo convencer as empresas a efetuarem esse procedimento de troca de número, e já vem se tornando relativamente famoso com o golpe do "Me empreste dinheiro?" no whatsapp (https://www1.folha.uol.com.br/cotidiano/2019/01/bandidos-clonam-contas-de-whatsapp-para-aplicar-golpes-veja-dicas.shtml)

Uma vez com o número clonado, o atacante instala o aplicativo (whatsapp ou telegram) em um novo celular e tenta utilizar o número e conta da vítima, que é identificada pelo seu número de telefone celular. O problema é que, por padrão, a única maneira que esses aplicativos utilizam para verificar se a pessoa que está instalando o aplicativo é de fato o dono da linha é enviando um código via mensagem SMS para o número cadastrado. Porém, como esse número foi clonado pelo atacante, ele recebe o código SMS e consegue instalar o aplicativo em um celular novo e ter acesso a todas as conversas da vítima.

O método explicado aqui neste manual acrescenta uma camada a mais de segurança nesse processo: a senha definida. Uma vez que seja feita essa configuração, o atacante não conseguirá mais ter acesso às mensagens apenas com o número que receberá via SMS, ele terá que informar, ainda, a senha que foi definida durante a configuração da autenticação de 2 etapas.

SESEI/TRF1