https://www.ctir.gov.br

14 de junho de 2019

Recomendação nº 04/2019 – *Como agir em caso de perfil falso em Redes Sociais (Telegram)*

Atualização: 14 de junho de 2019

Obs.: As informações aqui disponibilizadas têm o objetivo de fornecer avisos e recomendações sobre questões comuns de segurança da informação para integrantes de órgãos e entidades de governo e para o público em geral.

Dentro das trocas de informações entre CSIRTs, esta publicação está marcada como **TLP:WHITE***. Sujeitas às regras padrão de direitos autorais, as informações do TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**).

Por favor, entre em contato com o **CTIR Gov**, caso tenha alguma dúvida relacionada a esta publicação, por meio dos contatos a seguir.

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-2315

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

1. Descrição do Problema

Com bilhões de usuários ativos espalhados pelo mundo, no Brasil, aplicativos, como o ***Telegram***, figuram como as principais formas de expressão entre usuários de redes sociais. Em função dessa popularidade, eles estão sendo utilizados como instrumento estratégico de comunicação por integrantes de diversas empresas, inclusive com bastante difusão entre servidores públicos em todo o País e representações no exterior.

Páginas e contas que se fazem passar por outras pessoas não são permitidas. Ao verificar uma conta que finge ser você, alguém que você conhece ou uma figura pública, é recomendado que você denuncie imediatamente o eventual impostor a essas aplicações. Como consequência desse cenário, a difusão de perfis falsos pode ser particularmente danosa à imagem do servidor, seu cargo e ao seu respectivo órgão e, por mais que existam formas de combate às ações de falsidade ideológica, a penalização dos responsáveis pela criação de perfis falsos não é uma ação simples de se realizar.

O **CTIR Gov** recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, da presente recomendação, orientando quais são os recursos disponibilizados pelas plataformas para seus usuários ao se descobrir a existência de perfis falsos.

2. Impacto

A atribuição de falsidade ideológica na utilização de perfis falsos pode resultar em dano à imagem da pessoa cujo o perfil falso foi atribuído, assim como ao cargo que ocupa e ao órgão em que está lotada.

3. Recomendações

Denuncie o caso ao canal adequado disponível em cada uma das aplicações, enviando todas as informações solicitadas, incluindo uma foto do seu documento de identidade emitido pelo governo, exigida em alguns casos.

Como reforço, envie os dados de sua denúncia ao endereço eletrônico *ctir@ctir.gov.br*, para que o ***CTIR Gov*** também abra uma notificação junto à empresa e acompanhe as ocorrências entre integrantes de órgãos de governo e vinculados.

4. Formas de Denúncia

4.1. *Telegram* *https://telegram.org/faq/br*.

4.1.1. O que fazer no caso de celular roubado?

- A empresa informa que o número de telefone é a única maneira de identificar um usuário do ***Telegram***. Eles não coletam informações adicionais sobre o usuário, portanto, quem tiver o número tem a conta. Apenas conseguirão ajudar a menos que o usuário tenha acesso ao número de telefone ou ao próprio aplicativo do Telegram conectado na própria conta em qualquer um dos seus dispositivos.
- O usuário consegue acessar sua conta do ***Telegram*** por outro dispositivo.
    - Vá para *"Configurações do Telegram"* > "*Privacidade e Segurança*"> e ative a "*Verificação em Duas Etapas*". Dessa forma, o número de telefone, por si só, não será suficiente para fazer *login* na sua conta.
    - Vá para "*Configurações do Telegram*"> "*Privacidade e Segurança*" > "*Sessões Ativas*" e encerre a sessão do ***Telegram*** no dispositivo antigo. Quem tiver o telefone não poderá fazer *login* novamente, pois não sabe a senha.
    - Entre em contato com a operadora do serviço telefônico, para que bloqueiem o *chip* SIM antigo e emitam um novo com o seu número.
    - Se decidir mudar para um novo número de telefone, não esquecer de ir em "*Configurações do Telegram*", tocar no número de telefone e alterar o número do ***Telegram*** para o novo.
- O usuário não tem acesso ao ***Telegram*** em nenhum outro dispositivo.
    - Em primeiro lugar, o usuário precisa entrar em contato com a operadora do telefone para que bloqueiem o antigo *chip* SIM e emitam um novo com o número.
    - Ao receber o novo *chip* SIM com o número antigo, fazer o *login* no ***Telegram***, depois vá em "*Configurações do Telegram*"> "*Privacidade e Segurança*" > "*Sessões Ativas*" e encerrar a sessão do Telegram no dispositivo antigo.
- Removendo dados confidenciais.
    - O usuário pode apagar sua conta do ***Telegram*** se estiver logado em pelo menos um dos seus outros dispositivos (móvel ou desktop).
    - Observar que as contas inativas do ***Telegram*** se autodestroem automaticamente após um período de tempo (6 meses sendo a configuração padrão).

4.1.2. Como denunciar conteúdo irregular para a equipe de abuso do ***Telegram***

- ***Android***: abrir o canal, clicar em "..." no canto superior direito e depois em "*Denunciar*".
- ***iOS***: abrir o canal, clicar na imagem no canto superior direito para abrir o perfil. O botão "*Relatório*" está logo acima de "*Deixar canal*".
- ***Telegram Desktop***: abrir o perfil do canal. O botão "*Relatório*" está logo acima de "*Deixar canal*".
- Também poderá ser enviado um *e-mail* para *abuse@telegram.org* ou *dmca@telegram.org*. Certificar-se de incluir um *link* ou *@username* no conteúdo que está denunciando. Não há a possibilidade de se localizar entidades com base em capturas de tela.

5. Protegendo a sua conta: como ativar a autenticação de dois fatores

5.1. *Telegram* *https://telegram.org/faq/br*.

5.1.1. Como ativar a verificação em duas etapas no ***Telegram***

- Acessar "*Configurações do Telegram*"> selecionar a opção "*Privacidade e segurança*";
- Acessar o menu "*Verificação em duas etapas*"> clicar em "*Configurar senha adicional*";
- Definir uma senha de acesso ao ***Telegram*** e clicar no botão na parte de cima da tela para avançar. O aplicativo solicitará que seja digitada a chave mais uma vez para confirmar.
- Informar uma dica para recordação da combinação.
- Se solicitado um *e-mail* para apoio na recuperação da senha.
- Digitar o código enviado ao correio eletrônico informado para confirmação.
- Clicar uma última vez no botão com ícone de visto na parte de cima.
- Uma vez habilitada a dupla autenticação, é necessário um código *SMS* e também a senha para entrar.

5.1.2. O ***Telegram*** também conta com os *chats* secretos. As mensagens não são armazenadas na nuvem, só no celular ou computador onde o usuário as receber. Elas não podem ser encaminhadas e são eliminadas dos dois lados da conversa se o usuário a apagar do seu dispositivo.

5.1.3. Há ainda a opção de autodestruir texto, fotos, vídeos e arquivos após alguns segundos. O *timer* de autodestruição está disponível apenas para *chats* secretos.

- Para definir o *timer*, basta clicar no ícone de relógio (na caixa de texto no ***iOS***, ou na barra superior no ***Android***) e em "*Definir timer de autodestruição*"
- Configurar o limite de tempo desejado. O relógio começa a piscar no momento em que a mensagem é exibida na tela do destinatário (recebe dois *ticks* verdes). Assim que o tempo acabar, a mensagem desaparece de ambos os dispositivos.
- As fotos enviadas com *timers* de autodestruição curtos (<1 minuto) só podem ser visualizadas enquanto se está segurando o dedo nelas.
- O *timer* só se aplica a mensagens que foram enviadas após o temporizador ser definido. Não tem efeito nas mensagens anteriores.

6. Referências

- ***Alerta nº 02/2018 – Golpe de Clonagem de Contas do WhatsApp***. Disponível em: <*https://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_2018_02_whatsapp.pdf*> . Acesso em: 25 de fev. 2019.
- ***Recomendação nº 01/2018 - Golpe de Clonagem de Contas do Aplicativo WhatsApp***, com o detalhamento das medidas de prevenção e mitigação, publicada em: *https://www.ctir.gov.br/arquivos/recomendações/2018/Recomendação_1_2018_golpe_whatsapp.pdf*. Acesso em: 25 de fev. 2019.
- ***Telegram - Perguntas Frequentes***. Disponível em: <*https://telegram.org/faq/br*>. Acesso em: 13 de jun. 2019.

Coordenação-Geral do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR)

Informações: cgtir@presidencia.gov.br
Notificação de incidentes: ctir@ctir.gov.br