https://www.ctir.gov.br

23 de março de 2019

Recomendação nº 02/2019 – *Como agir em caso de perfil falso em Redes Sociais* *(Facebook, WhatsApp e Instagram)*

Atualização: 14 de junho de 2018

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

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.

1. Descrição do Problema

Com bilhões de usuários ativos espalhados pelo mundo, no Brasil, aplicativos como ***Facebook, WhatsApp e Instagram*** 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**, contando também com informações cedidas gentilmente pela Gerência de Políticas Públicas do ***Facebook***, 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 perfil falso foi atribuído, assim como ao cargo que ocupa e ao órgão em que está lotada.

3. Recomendações

Denunciar 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.

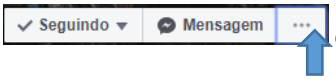
Como reforço, enviar os dados de sua denúncia ao endereço eletrônico *ctir@ctir.gov.br*, para que o **CTIR Gov** também abra uma notificação junto à empresa e acompanhe as ocorrências entre integrantes de órgãos de governo e vinculados.

4. Formas de Denúncia

4.1 *Facebook*

4.1.1. Se quiser denunciar uma conta por se passar por outra pessoa, primeiro determinar se a denúncia se refere a um Perfil ou uma Página, entenda a diferença no *link https://www.facebook.com/help/337881706729661?helpref=faq_content*.

4.1.2. Para denunciar um Perfil, vá até a conta impostora. Se não for possível encontrá-lo, experimente pesquisar o nome usado no perfil ou perguntar a amigos se eles podem lhe enviar um *link*.

4.1.3. No perfil a ser denunciado, Clique no botão *"..."*, ao lado de *"Mensagem "* 

e, em seguida, em *"Dar feedback ou denunciar esse perfil"*.

4.1.4. Siga as instruções na tela para enviar a denúncia sobre imitação de identidade.

4.1.5. Caso não tenha uma conta do ***Facebook*** e precise denunciar alguém que está fingindo ser você ou uma pessoa que você conhece, preencha o formulário no *link* *https://www.facebook.com/help/contact/295309487309948?helpref=faq_content*.

4.1.6. Para denunciar uma Página do ***Facebook*** que esteja se passando por uma figura pública, preencha o formulário no link *https://www.facebook.com/help/contact/2047597315284384?helpref=faq_content*.

4.1.7. Se a conta que se passa por outra pessoa estiver apenas no ***Messenger***, abra a conversa e toque em (***Android***) ou no nome da pessoa, na parte superior (***iPhone/iPad***); role a tela para baixo e toque em *"Ocorreu um erro"*; selecione *"Fingindo ser outra pessoa"* como sua categoria; toque em *"Enviar feedback"*; toque em *"Denunciar conversa > Denunciar"* para enviar a conversa para análise.

4.1.8. A sua denúncia está feita e será analisada pela equipe do ***Facebook***. Enquanto isso, você poderá verificar o *status* da denúncia na *"Caixa de Entrada de Suporte"* (*https://www.facebook.com/support/).*

4.2 *WhatsApp*

4.2.1. Com a conversa (do grupo ou de uma pessoa) aberta, clicar no botão com três pontos no canto superior direito;

4.2.2. No menu, clicar em *"Mais"*;

4.2.3. A seguir, clicar na opção *"Denunciar"*;

4.2.4. Caso não deseje apagar as mensagens recebidas e sair do grupo ou bloquear o contato em questão, desmarque a caixa indicada antes de concluir o processo clicando em *"Denunciar"*.

Observação:

- O ***CTIR Gov*** também recomenda a leitura da 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/alertas/2018/recomendacao_2018_01_whatsapp.pdf*.

4.3. *Instagram*

4.3.1. Clicar no link *http://help.instagram.com/contact/636276399721841?helpref=faq_content* e preencher o formulário com suas informações pessoais.

4.3.2. A denúncia também poderá ser feita diretamente no aplicativo. Vá ao perfil da conta que está se fazendo passar por você ou alguém que você conheça e clique em "...", e em seguida, denunciar, no canto superior direito. Seguir os passos.

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

5.1. Facebook (*https://www.facebook.com/help/148233965247823*)

5.1.1. A autenticação de dois fatores é um recurso de segurança que ajuda a proteger a conta do ***Facebook***, além da senha.

5.1.2. Se o usuário configurou a autenticação de dois fatores, será solicitado que insira um código de *login* especial ou confirme a tentativa de acesso todas as vezes que alguém tentar acessar o ***Facebook*** de um computador ou dispositivo móvel que não sejam reconhecidos. Também há a possibilidade de se receber alertas quando alguém tentar entrar na sua conta usando um computador que não seja reconhecido.

5.1.3. Como ativar ou gerenciar a autenticação de dois fatores:

- Vá até Configurações de segurança e *login* clicando em (símbolo) no canto superior direito do Facebook e em **Configurações > Segurança > *login***.
- Role a tela para baixo para **Usar autenticação de dois fatores** e clique em **Editar**.
- Escolha o método de autenticação que deseja adicionar e siga as instruções na tela.
- Clique em **Ativar** depois de ter selecionado e ativado um método de autenticação.

5.2. WhatsApp (*https://faq.whatsapp.com/pt_br/android/26000021/*)

5.2.1. A Verificação em duas etapas é um recurso opcional para adicionar ainda mais segurança à conta. Ao ativar a verificação em duas etapas, qualquer tentativa de verificação do seu número de telefone no ***WhatsApp*** terá de ser acompanhada por um PIN de seis dígitos criado por você através deste recurso.

5.2.2. Para ativar a verificação em duas etapas, abra o **WhatsApp > Configurações > Conta > Verificação em duas etapas > Ativar**.

5.2.3. Ao ativar este recurso, haverá a opção de se inserir o endereço de *e-mail*. Este endereço de *e-mail* será utilizado para que o ***WhatsApp*** possa enviar ao usuário um *link* para desativar a verificação em duas etapas caso se esqueça o PIN e para ajudar a proteger a conta. Não há a verificação deste endereço de *e-mail* para confirmar sua autenticidade. Recomenda-se que se forneça um endereço de *e-mail* autêntico, pois assim se reduz o risco de ficar sem acesso à conta caso esqueça o PIN.

Importante: Se receber um *e-mail* para desativar a verificação em duas etapas sem tê-la solicitado, não clicar neste *link*. Outra pessoa pode estar tentando registrar o seu número no WhatsApp.

5.2.4. Para ajudá-lo a se lembrar do seu PIN, o ***WhatsApp*** irá solicitar que o digite periodicamente. Não há como desativar essa solicitação sem que a verificação em duas etapas em si também seja desativada.

Observação: No ***WhatsApp***, o histórico de mensagens, quando acionado o *backup*, fica guardado no ***Google Drive*** (***Android***) ou ***iCloud*** (***iOS***). Para acessá-lo, é necessário ter a senha da conta ***Google*** ou do ***Apple ID***. Dessa forma, é possível acessar a conta de outra pessoa roubando seu número de celular, mas não será o bastante para ler as conversas antigas do usuário.

5.3. *Instagram* (*https://help.instagram.com/566810106808145?helpref=page_content*)

5.3.1. A autenticação de dois fatores é um recurso de segurança. Se tiver configurado a autenticação de dois fatores, será solicitado inserir um código de *login* especial ou confirmar a tentativa de acesso todas as vezes que alguém tentar acessar o Instagram de um dispositivo que não seja reconhecido.

5.3.2. Há vários métodos de autenticação de dois fatores que podem ser usados com a conta do Instagram. Para começar a usar a autenticação de dois fatores, escolher entre "Códigos de mensagem de texto (SMS) no celular" e "Códigos de *login* de um aplicativo de autenticação de terceiros (como o *Duo Mobile ou o Google Authenticator*)".

5.3.2. Será necessário configurar pelo menos um destes para poder usar a autenticação de dois fatores.

Observação: depois de ativar a autenticação de dois fatores, você poderá acessar os códigos de recuperação de sua conta, caso tenha problemas para recuperar um código.

6. Referências

- Central de Ajuda do ***Facebook*** - Como faço para denunciar uma conta ou uma Página que está fingindo ser eu ou outra pessoa? - Disponível em: *https://www.facebook.com/help/174210519303259*. Acesso em: 25 de fev. 2019.
- Suporte do ***WhatsApp*** - *Stolen Accounts* - Disponível em: *https://faq.whatsapp.com/pt_pt/general/26000244/?category=5245246*. Acesso em: 25 de fev. 2019.
- Central de Ajuda do ***Instagram*** - Denunciar uma conta impostora no Instagram - Disponível em: *https://help.instagram.com/contact/636276399721841?helpref=faq_content*. Acesso em: 25 de fev. 2019.
- ***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.
- Fique seguro no ***WhatsApp***. Disponível em: <*https://faq.whatsapp.com/pt_br/android/21197244/?category=5245250*>. Acesso em: 25 fev. 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