https://www.ctir.gov.br

23 de março de 2019

Recomendação nº 03/2019 – *Como agir em caso de perfil falso em Redes Sociais (Twitter)*

Atualização: 14 de junho de 2019

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.

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**).

1. Descrição do Problema

Com bilhões de usuários ativos espalhados pelo mundo, no Brasil, aplicativos, como o ***Twitter***, 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. *Twitter*

4.1.1. Clique no link *https://help.twitter.com/forms/impersonation* .

4.1.2. Na página, se poderá marcar detalhes sobre o pedido de ajuda. Entre as opções, *"Uma conta está se passando por mim ou por alguém que eu conheço"; "Uma conta está fingindo ser ou representar minha empresa, marca ou organização"; "Minha conta foi suspensa"; "Não consigo entrar em minha conta"; "Minha conta foi invadida ou comprometida";* e *"Alguém está usando meu endereço de e-mail sem minha permissão";*

4.1.3. Escolher a opção e, em seguida, seguir as instruções na tela para enviar a denúncia.

5. Protegendo a sua conta: como ativar a autenticação de dois fatores (verificação de acesso)

5.1. *Twitter* (*https://help.twitter.com/pt/managing-your-account/two-factor-authentication*)

5.1.1. A verificação de acesso é uma camada adicional de segurança para sua conta do ***Twitter***. Em vez de inserir somente uma senha para entrar, o usuário também fornecerá um código que é enviado para o seu celular. Essa verificação ajuda a garantir que o usuário, e mais ninguém, tenha acesso à sua conta.

5.1.2. Depois de ativar essa função, o usuário precisará da senha e do número do celular ou de uma chave de segurança (pelo *twitter.com*) para entrar em sua conta. Quando entrar no *twitter.com*, no ***Twitter*** para ***iOS***, no ***Twitter*** para ***Android*** ou no *mobile.twitter.com*, receberá um código de acesso de seis dígitos para ser inserido. Por padrão, ele será enviado por mensagem de texto SMS (consultar a lista de operadoras com suporte em: *https://help.twitter.com/pt/using-twitter/supported-mobile-carriers*) ou poderá usar um aplicativo de terceiros ou uma chave de segurança para a verificação (veja os detalhes abaixo).

Observação: Para configurar a verificação de acesso, é preciso ter um número de celular associado à sua conta do ***Twitter***. Essa exigência existe para a recuperação da conta. Se o usuário gerenciar várias contas que usam o mesmo número de celular, é possível usar a verificação de acesso para cada conta. Para aumentar a segurança, se recomenda ativar a verificação de acesso em todas as contas.

5.1.3. Como verificar seu acesso

Aqui apresentamos as opções de configuração no twitter.com, caso deseje verificar as formas específicas para ***iOS*** ou ***Android***, selecionar o ícone e clicar -> 

- Para configurar a verificação de acesso no *twitter.com*:
  - No menu superior, clicar no ícone do *"perfil*" e depois em "*Configurações*" e "*privacidade*".
  - Clicar nas configurações da "*Conta"* (*https://twitter.com/settings/account*) e em "*Configurar verificação de acesso*".
  - Ler as instruções da visão geral e clicar em "*Iniciar*".
  - Digitar a senha e clicar em "*Verificar*".
  - Clicar em "*Enviar código*" para adicionar o número de celular.

    Observação: se o usuário já tiver um número de celular associado à sua conta do ***Twitter***, receberá um SMS para confirmar o número.
  - Inserir o código de verificação enviado para o dispositivo e clicar em "*Enviar*".
  - Clicar em "*Obter código de backup"* para visualizar um código gerado pelo ***Twitter***.

    Recomenda-se guardar uma captura de tela do código, para o caso de se precisar dele no futuro. Assim, o usuário poderá acessar sua conta, se perder o aparelho ou mudar o número do celular.
  - Agora, quando o usuário entrar em sua conta no *twitter.com*, no ***Twitter*** para ***iOS***, no ***Twitter*** para ***Android*** ou no *mobile.twitter.com*, um código de acesso de seis dígitos será enviado para o seu telefone via mensagem de texto. Quando solicitado, inserir o código para acessar a sua conta.

- Para escolher o tipo de verificação de acesso no *twitter.com* (o usuário pode optar por usar um aplicativo de terceiros ou uma chave de segurança para gerar um código de acesso):
  - No menu superior, clicar no ícone do *"perfil"* e depois em *"Configurações e privacidade"*.
  - Clicar em "*Conta"* e em "*Segurança"*.
  - A opção "*Mensagem de texto"* estará ativada por padrão. Clicar em "*Editar"* para não receber mais códigos por mensagem de texto. Se a seleção "*Aplicativo de segurança móvel"* ou "*Chave de segurança"* estiver desativada, será solicitado que o usuário a ative.

- Para configurar o uso de um aplicativo de terceiros para a verificação no twitter.com (O usuário pode usar um aplicativo autenticador de terceiros, como o ***Google Authenticator***, o ***Duo Mobile***, o ***Authy*** ou outro semelhante, instalado em seu dispositivo móvel):
  - No menu superior, clicar no ícone do "*perfil"* e depois em "*Configurações"* e "*privacidade"*.
  - Clicar na aba "*Conta"*.
  - Em "*Segurança"* e ao lado de "*Verificação de acesso"*, clicar no botão "*Revise seus métodos de verificação de acesso"* para começar.
  - Digitar a senha e clicar em "*Confirmar"*.
  - A partir das seleções, clicar em "*Configurar"* ao lado de "*Aplicativo de segurança móvel"*.
  - Ler as instruções e clicar em "*Iniciar"*.
  - Se for solicitado que se verifique a senha, inseri-la e clicar em "*Verificar"*.
  - Surgirá uma janela *pop-up* que exibe um "*Código QR"*. Seguir as instruções descritas.
  - Para configurar o aplicativo autenticador de terceiros, será necessário digitalizar o Código QR. Em seguida, aparecerá um código de segurança numérico de 6 dígitos.
  - Inserir esse código no campo de texto "*Código de segurança"* na janela *pop-up*.
  - Clicar em "*Concluído"*.

- Para configurar o uso de uma chave de segurança para a verificação no twitter.com (O usuário pode usar uma chave de segurança USB, como uma ***Yubikey***, ou semelhante):
  - No menu superior, clicar no ícone do "*perfil"* e depois em "*Configurações"* e "*privacidade"*.
  - Clicar na aba "*Conta"*.
  - Em "*Segurança"* e ao lado de "*Verificação de acesso"*, clicar no botão "*Revise seus métodos de verificação de acesso"* para começar.
  - Digitar a senha e clicar em "*Confirmar"*.
  - A partir das seleções, clicar em "*Configurar"* ao lado de "*Chave de segurança"*.

- Ler as instruções e clique em "*Iniciar*".
- Se for solicitado que se verifique a senha, inseri-la e clicar em "*Verificar*".
- Uma janela *pop-up* será exibida pedindo que se registre a chave inserindo-a na porta USB do computador. Depois de inseri-la, pressionar o botão localizado na chave. Em seguida, verificar a chave pressionando o botão mais uma vez.

  Importante: o usuário também deve ter a opção "*Mensagem de texto*" ou "*Aplicativo de segurança móvel*" ativada para a verificação de acesso. Não é possível ativar a "*Chave de segurança*" por si só.

6. Referências

- Central de Ajuda do ***Twitter*** - Denunciar uma conta por falsa identidade. Disponível em: *https://help.twitter.com/forms/impersonation*. Acesso em: 25 de fev. 2019.
- Central de Ajuda do ***Twitter*** - Como usar a verificação de acesso. Disponível em: *https://help.twitter.com/pt/managing-your-account/two-factor-authentication*. Acesso em: 13 de jun. 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