https://www.ctir.gov.br

14 de junho de 2019

Recomendação nº 05/2019 – *Como agir em caso de clonagem do celular*

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.

1. Descrição do Problema

Se trata de um aparelho que foi reprogramado para transmitir o código do aparelho e o código de um assinante habilitado. Um fraudador pode usar um aparelho clonado para fazer ligações debitadas na conta de um titular regular da linha. É possível clonar um *chip* a partir do contato físico com o cartão SIM original. Com acesso ao aparelho, basta remover o *chip* original e inseri-lo em um dispositivo preparado para clonagem junto a um *chip* novo. Dessa forma os dados podem ser rapidamente transferidos.

Casos de furto de celular e tentativas de *hackeamento* das contas são cada vez mais praticados. A troca do *chip* para um outro aparelho pode proporcionar o acesso e posse de aplicativos como o ***WhatsApp*** para se entrar em contato com amigos e familiares para, por exemplo, pedir dinheiro se passando pela vítima do golpe. Existem também formas de interceptar conversas em aplicativos como o ***Telegram*** e o ***WhatsApp***. Um dos golpes é o *SIM Swap*, quando o autor da atividade maliciosa clona o cartão de operadora (SIM) da vítima, o que pode ser feito com algum criminoso infiltrado na empresa telefônica ou por meio das chamadas com o objetivo de engenharia social.

O **CTIR Gov** recomenda a divulgação, em todos os órgãos de governo e entidades vinculadas, da presente recomendação, orientando quais são os recursos disponibilizados para a prevenção, verificação e mitigação de incidentes relacionados ao tema.

2. Impacto

Débitos de prestação de serviços acima da média e consequentes atribuições de falsidade ideológica na utilização de perfis falsos, resultantes da perda da posse o aparelho celular, podem resultar em danos à imagem da vítima, assim como ao cargo que ocupa e ao órgão em que está lotada.

3. Recomendações

Atentar para as recomendações de prevenção e mitigação do problema que constam nesta publicação e, como reforço, siga as recomendações previstas para os casos de perfis falsos em Redes Sociais que se encontram na seção “Alertas e Recomendações” no site do ***CTIR Gov*** (*https://www.ctir.gov.br/alertas/*).

4. Medidas de Segurança

4.1 Prevenção - Com a posse do telefone

4.1.1. Utilizar código alfanumérico (letras e números) para bloqueio de celular. Padrões de desenho (em Android) ou códigos numéricos como "1234", "0000", ou parecidos, se mostram ineficientes.

4.1.2. Habilitar a biometria ou senha para todos os aplicativos que suportam tais facilidades, como os aplicativos de banco.

4.1.3. Utilizar autenticação de dois fatores em todas as contas de redes sociais e serviços de Internet (***Facebook***, ***Instagram***, ***Gmail***, etc), mas nunca por SMS, pois perderá efeito no caso de roubo do celular.

- Para saber como, consulte as recomendações “*Como agir em caso de perfil falso em Redes Sociais*” acessando *https://www.ctir.gov.br/alertas/*.

4.1.4. Desabilitar as notificações na tela de bloqueio do celular.

- Como desativar notificações na tela de bloqueio do ***iPhone***
  - Para visualizar as notificações na tela bloqueada sem desbloquear o seu iPhone, seguir as instruções: Vá em Ajustes > Notificações > Mostrar Pré-visualizações > e selecionar Sempre. Para impedir que isso aconteça, selecione apenas *“Quando desbloqueado”* ou *“Nunca”*.
- Como desativar notificações na tela de bloqueio do ***Android***
  - As configurações do ***Android*** costumam variar um pouco dependendo da versão e do smartphone. Porém, como padrão, pode-se encontrar as opções seguindo as instruções: abra as Configurações > busque por Apps e Notificações (ou apenas Notificações) > escolha tela de bloqueio > Defina para *“Não exibir notificações”* ou *“Ocultar conteúdo”*.

4.1.4. Anotar a marca, modelo, IMEI e número de série do aparelho em algum lugar. Também o PIN e PUK do chip (registrados no cartão do *chip*).

- O *chip* costuma vir em um envelope ou cartão, contendo informações importantes. É o caso do PIN e do PUK, dois códigos para a garantia da segurança do aparelho, que servem para impedir o uso do *chip* por terceiros.
- O código PIN é utilizado como senha de desbloqueio do *chip*, mas essa função normalmente vem desativada pelas operadoras. O código PUK é a senha utilizada para liberar o PIN. Caso se digite o código PIN errado muitas vezes, o *chip* será bloqueado e para desbloqueá-lo será necessário digitar o código PUK.

4.1.5. Habilitar o PIN do *chip*. Ao ativar o código, para se acessar o *chip* ou informações contidas nele, como contatos, será solicitado o PIN.

- O *chip* já vem com um PIN da operadora, que se recomenda alterar. Os padrões são: Vivo (8486); TIM (1010); Claro (3636); e Oi (8888).
- Para ativar o código PIN, entre em configurações do *smartphone* > procure a opção *"Segurança"* e acesse > encontre a opção *"Configurar bloqueio do SIM"* > preencha ou ative a função *"Bloquear cartão SIM"* > será solicitado o código PIN padrão. Caso nunca o tenha alterado, coloque o código referente à sua operadora citado no tópico acima.
- Para alterar o código PIN, o usuário encontrará a opção de "*Alterar PIN do SIM"* e nela vai poder alterar o código PIN para um número com 4 dígitos que desejar.
    - Se esquecer o código PIN e errar várias vezes (normalmente 03), o *chip* será bloqueado e para desbloqueá-lo, deverá usado o código PUK.
    - Caso digite o PUK errado por 10 vezes, o *chip* será bloqueado definitivamente, devendo ser adquirido um novo *chip,* porém poderá continuar utilizando o número antigo, justamente por que o PUK bloqueado é impossível de ser recuperado.
- Caso não tenha os números em mãos, basta entrar em contato com a central de atendimento da operadora, para solicitar o código PIN e PUK. O *chip* deve estar cadastrado e somente o titular da linha pode fazer a solicitação do código.

4.2 Mitigação - Após o roubo, furto ou perda do aparelho celular

4.2.1. Atentar para o fato de que, quanto mais tempo se deixar o *chip* habilitado, mais tempo haverá para a execução da fraude.

4.2.1. Ligar para a operadora e informar o ocorrido, para o bloqueio do *chip*.

4.2.2. Fazer um boletim de ocorrência na delegacia mais próxima ou pela *Internet*. Serão necessários os números do IMEI e de série do aparelho.

4.2.3. Desconectar o dispositivo das contas de *e-mail*, redes sociais e outros serviços (***Gmail***, ***Facebook***, ***Instagram***, ***Twitter***...)

- Para saber como, consulte as recomendações "*Como agir em caso de perfil falso em Redes Sociais*" acessando *https://www.ctir.gov.br/alertas/*.

4.2.3. Programar a exclusão dos dados pelo site do fabricante (***Google***, ***Apple***, ...).

Observações:

- Importante frisar que, conforme consta nas orientações da ***Agência Nacional de Telecomunicações (Anatel)***, a vítima de celular clonado deve comunicar à operadora telefônica e pedir o bloqueio da linha, além de solicitar esclarecimentos sobre o que foi registrado no caso.
- A ***Anatel*** também orienta sobre indícios que podem indicar que um celular foi clonado: dificuldades para completar chamadas originadas; quedas frequentes de ligação; dificuldade para acesso à caixa de mensagem; chamadas recebidas de números desconhecidos, nacional e internacional; e débitos de prestação de serviços muito acima da média.

5. Referências

- ***Tudo sobre Segurança – Você sabe o "IMEI" do seu celular?*** Disponível em: <*http://tudosobreseguranca.com.br/portal/index.php?option=com_content&task=view&id=841&Itemid=126%201/3*> . Acesso em 11 de jun. 2019.
- ***Mente Binária. O que fazer antes que seu celular seja roubado.*** Disponível em: <*https://www.mentebinaria.com.br/artigos/o-que-fazer-antes-que-seu-celular-seja-roubado-r44/*>. Acesso em: 14 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.
- ***ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES***. Disponível em: < *http://www.anatel.gov.br/institucional/*> Acesso em: 05 abr. 2018.
- ***Portal de Planos - PIN e PUK – Veja como descobrir esses códigos do seu SIM CARD e como usá-los.*** Disponível em: <*https://portaldeplanos.com.br/pin-e-puk/*>. Acesso em: 13 de jun. 2019.

Tecnoblog - Como reforçar a segurança da verificação em duas etapas. Disponível em: <*https://tecnoblog.net/267624/como-reforcar-a-seguranca-da-verificacao-em-duas-etapas/*>. Acesso em: 13 de jun. 2019.