

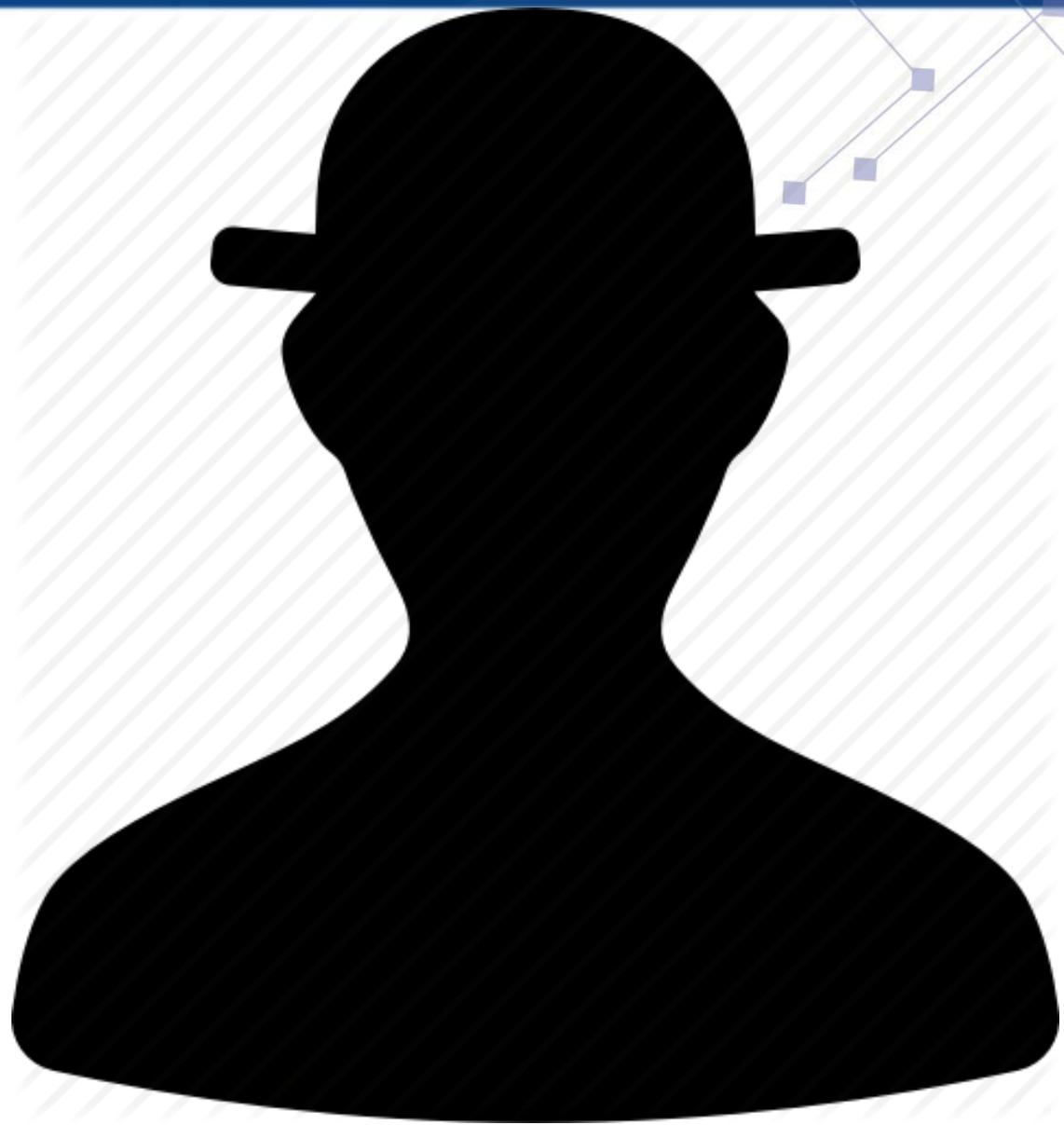
# 10 motivos para voltar ao tijolão

**CAIS – Centro de Atendimento a Incidentes de Segurança**  
**RNP – Rede Nacional de Ensino e Pesquisa**

## Whoami

*Yuri Alexandro*

- ✓ Analista de Sistemas
- ✓ Especialista em Gestão de Segurança da Informação
- ✓ 18 anos na área de TI
- ✓ 10 anos na área de Segurança da Informação
- ✓ Atualmente no CAIS/RNP



## e o CAIS?



- ✓ Missão: Zelar pela segurança da informação na rede acadêmica.
- ✓ Detecta incidentes de segurança.
- ✓ Alerta sobre vulnerabilidades.
- ✓ **Conscientização em segurança da informação.**



**E QUEM FORNECE ESSAS INFORMAÇÕES MUNDO AFORA?**





# 10

MOTIVOS PARA TER  
DE NOVO UM CELULAR

TIJO LÃO



# MOTIVO 1

# Tijolão é item de moda



# MOTIVO 2

# Tijolão não precisa ter senha

## Motivo 2: Tijolão não precisa ter senha



## Motivo 2: Tijolão não precisa ter senha



## Só ter senha resolve?

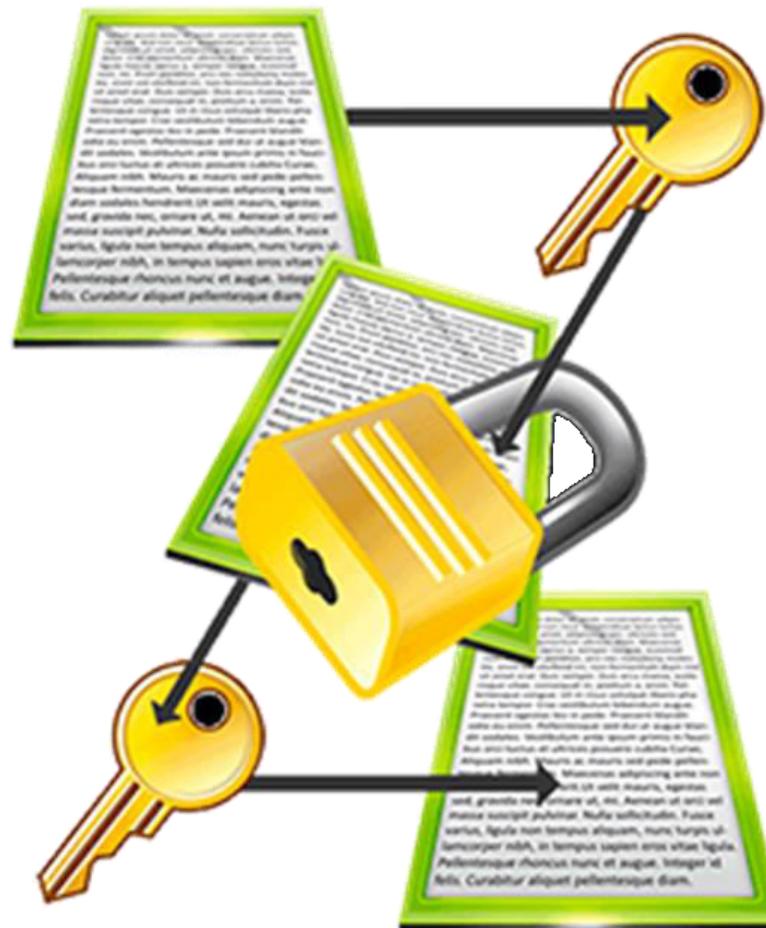
Cifragem dos dados

Apagar dados remotamente

# Só ter senha resolve?

## Cifragem dos dados

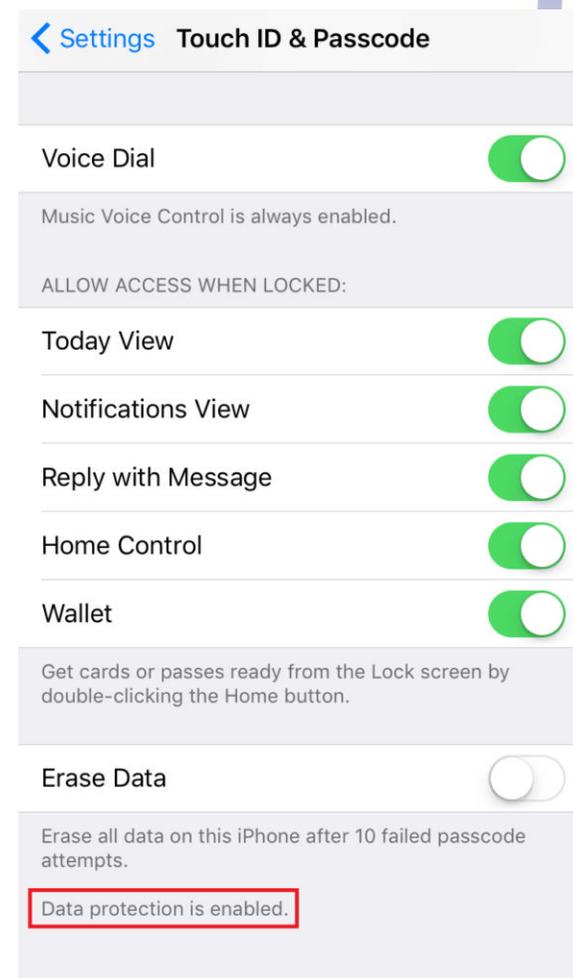
## Apagar dados remotamente



# Só ter senha resolve?

Cifragem dos dados [1] [2]

Apagar dados remotamente



# Só ter senha resolve?

Cifragem dos dados

Apagar dados remotamente

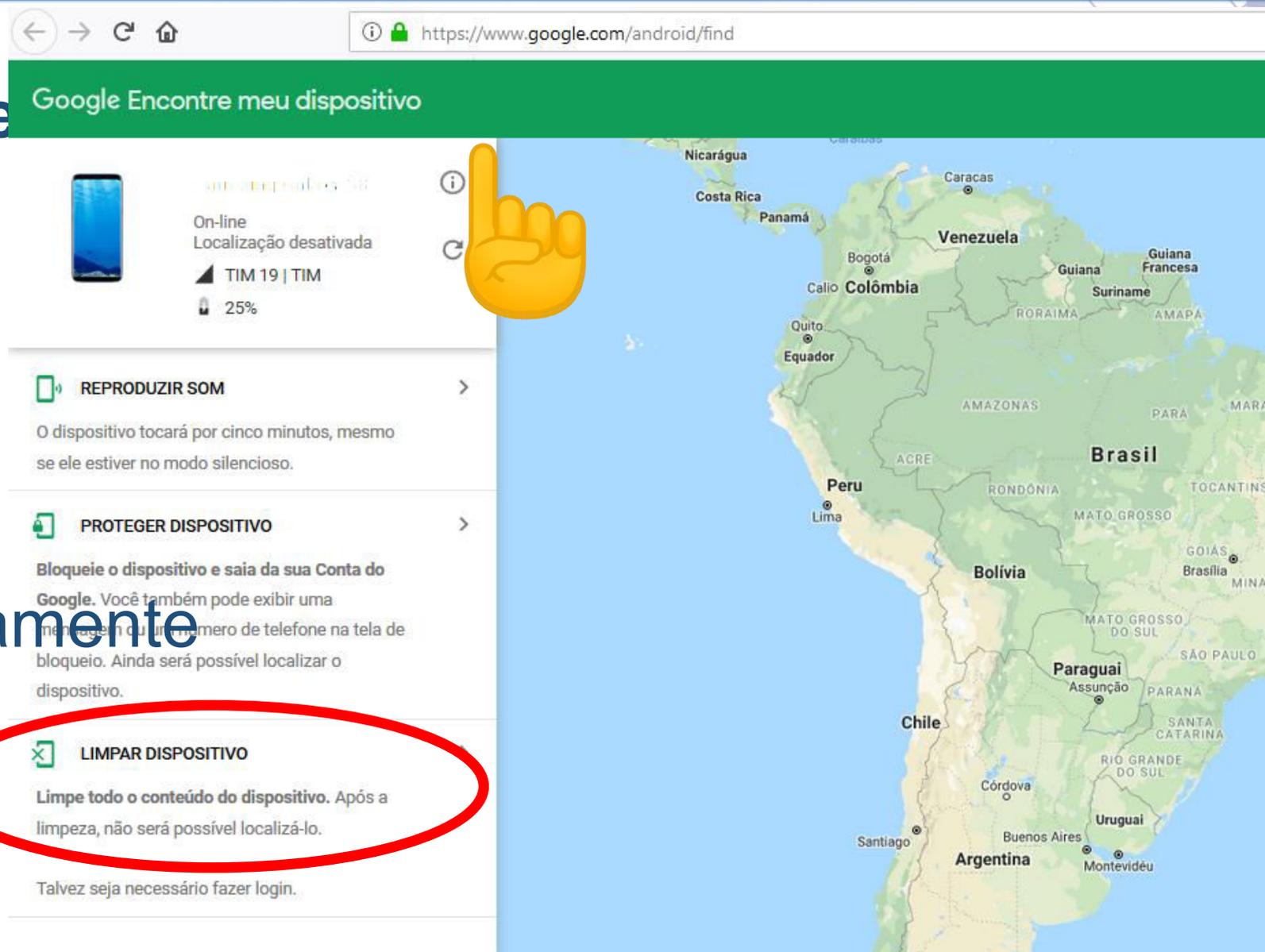


## Só ter senha resolve

## Cifragem dos dados

## Apagar dados remotamente

<https://www.google.com/android/find>



Google Encontre meu dispositivo

On-line  
Localização desativada  
TIM 19 | TIM  
25%

- REPRODUZIR SOM  
O dispositivo tocará por cinco minutos, mesmo se ele estiver no modo silencioso.
- PROTEGER DISPOSITIVO  
Bloqueie o dispositivo e saia da sua Conta do Google. Você também pode exibir uma mensagem ou um número de telefone na tela de bloqueio. Ainda será possível localizar o dispositivo.
- LIMPAR DISPOSITIVO**  
Limpe todo o conteúdo do dispositivo. Após a limpeza, não será possível localizá-lo.

Talvez seja necessário fazer login.

<https://www.google.com/android/find>

## Só ter senha resolve?

Cifragem dos dados

## Apagar dados remotamente

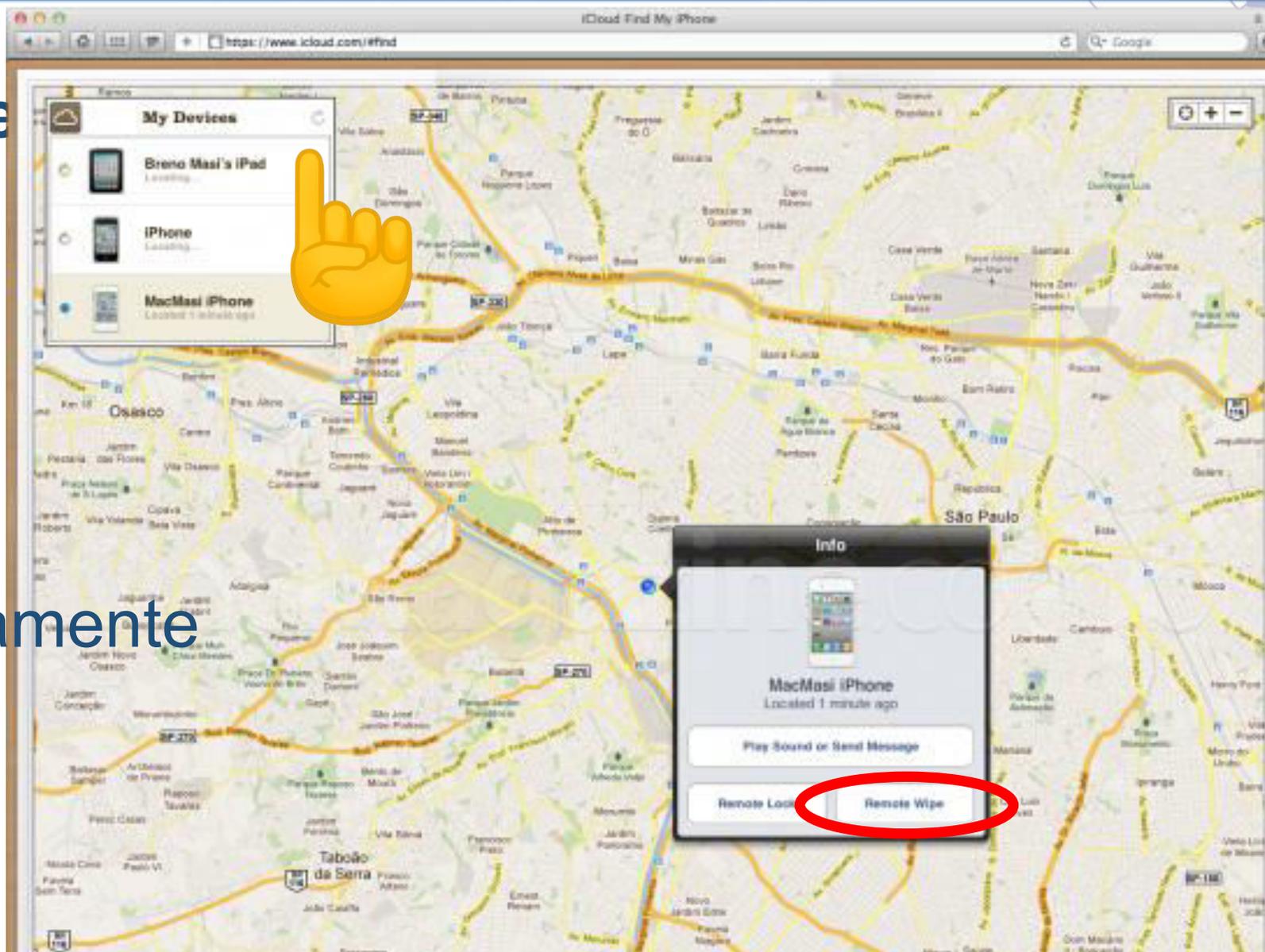


Só ter senha resolve

Cifragem dos dados

Apagar dados remotamente

<https://www.icloud.com/#find>



## Só ter senha resolve?

Cifragem dos dados

Apagar dados remotamente

## Outros softwares



etc.

# MOTIVO 3

## Tijolão inspirou o Highlander

**CAI NO CHÃO**



**QUEBRA A TELA**

**CAI NO CHÃO**



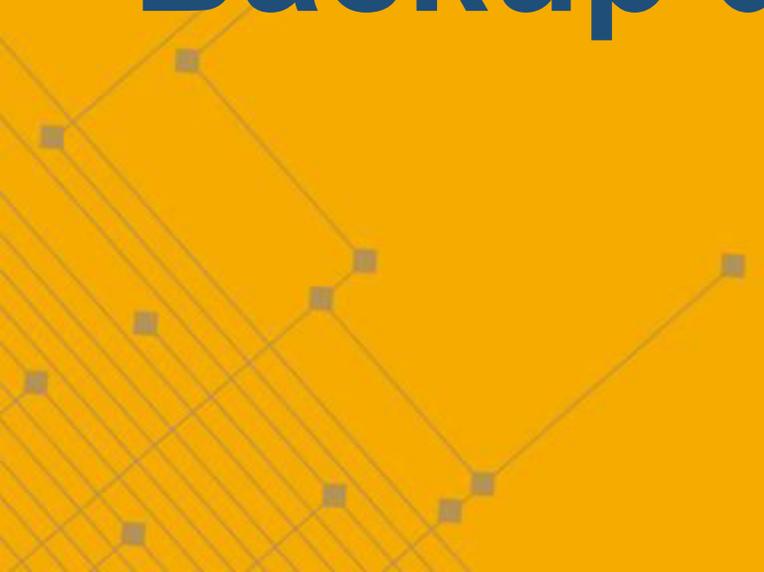
**QUEBRA O CHÃO**



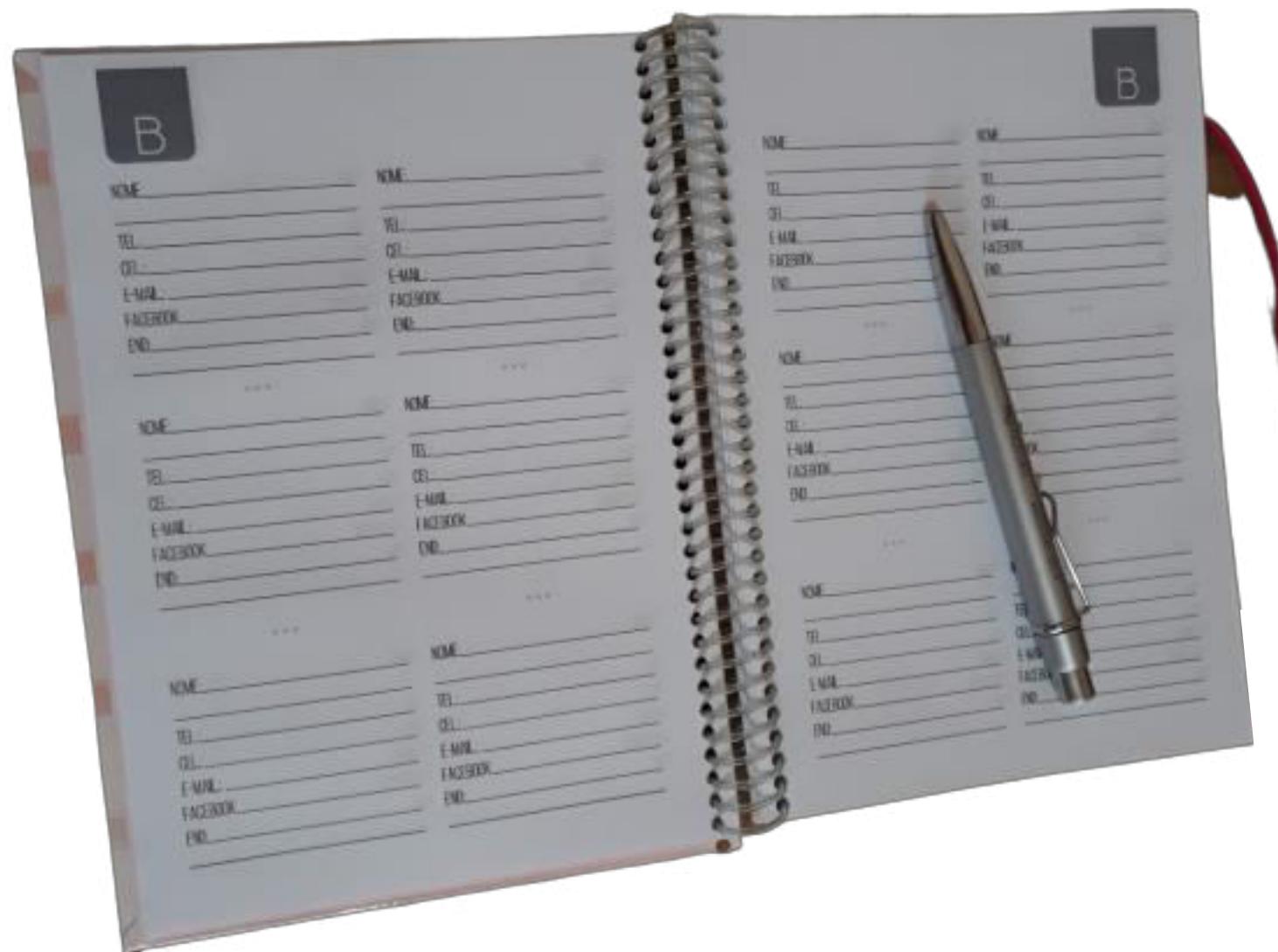
**VÔ, CONTA AQUELA VEZ QUE VOCÊ CAIU SEM CAPINHA DO SEGUNDO ANDAR E NEM TRINCOU**

# MOTIVO 4

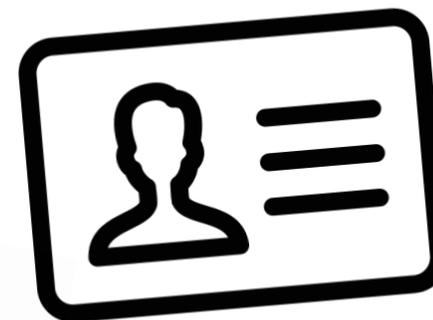
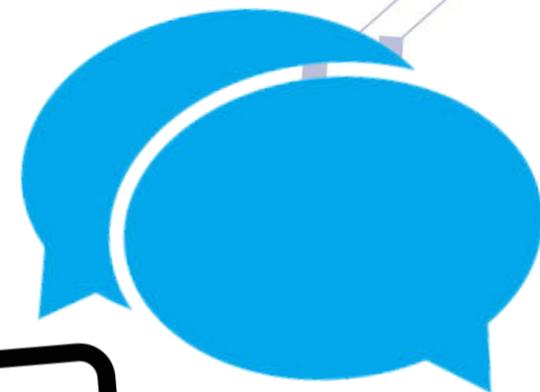
**Backup do tijolão é mais simples**

A decorative geometric pattern in the bottom-left corner, consisting of a grid of thin lines and small squares, creating a perspective effect.

## Com tijolão



## Com Smartphone





etc.



### Alguns cuidados ao colocar arquivos em nuvem

- ✓ Senha para acesso nos apps de nuvem
- ⊗ Senhas fáceis/óbvias
- ✓ Duplo fator de autenticação
- ✓ Dados cifrados
- ⊗ Guardar todos os arquivos na nuvem
- ⊗ App logado ou com senha gravada

# MOTIVO 5

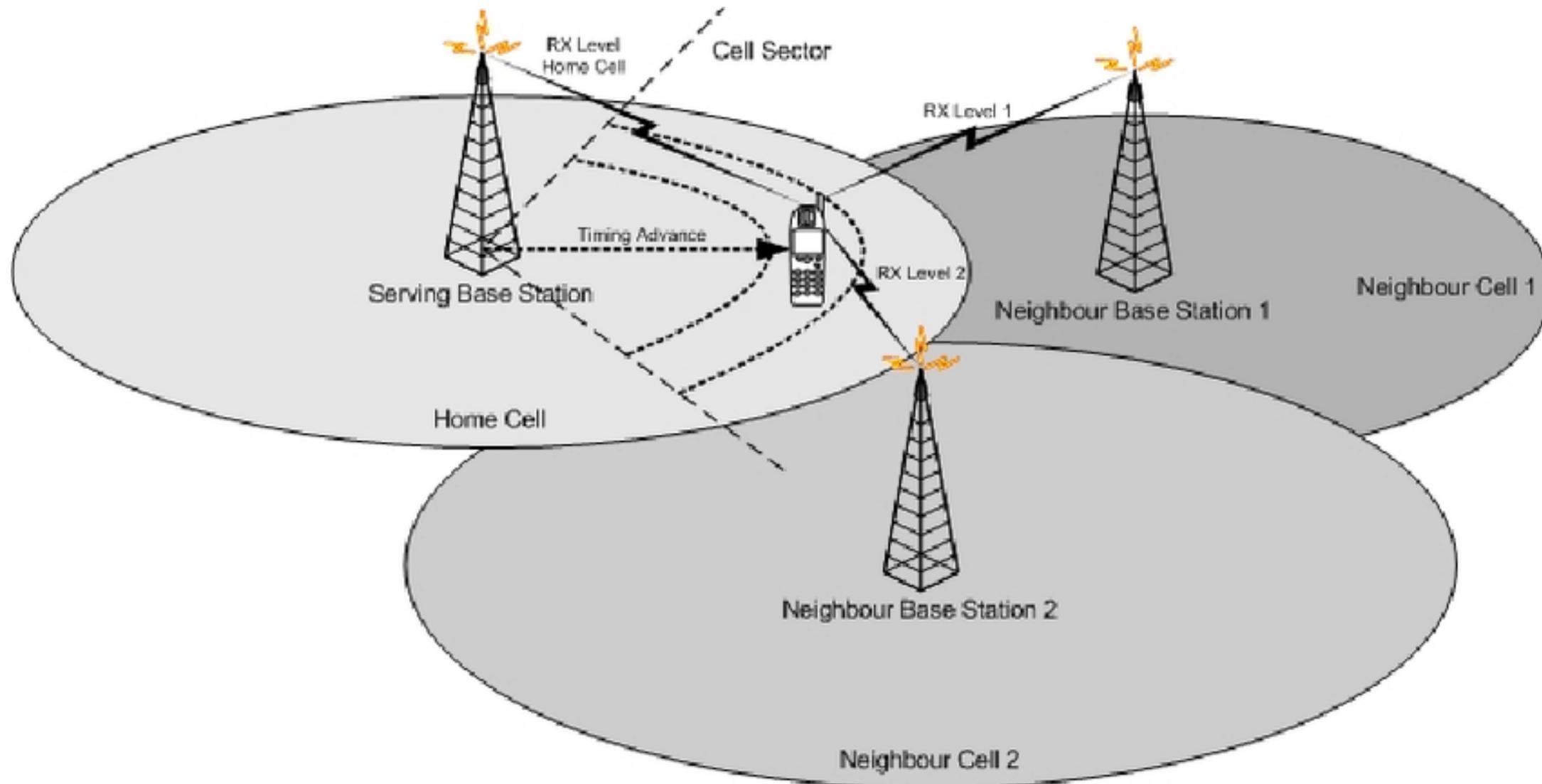
**Com tijolão, ninguém sabe onde você está**

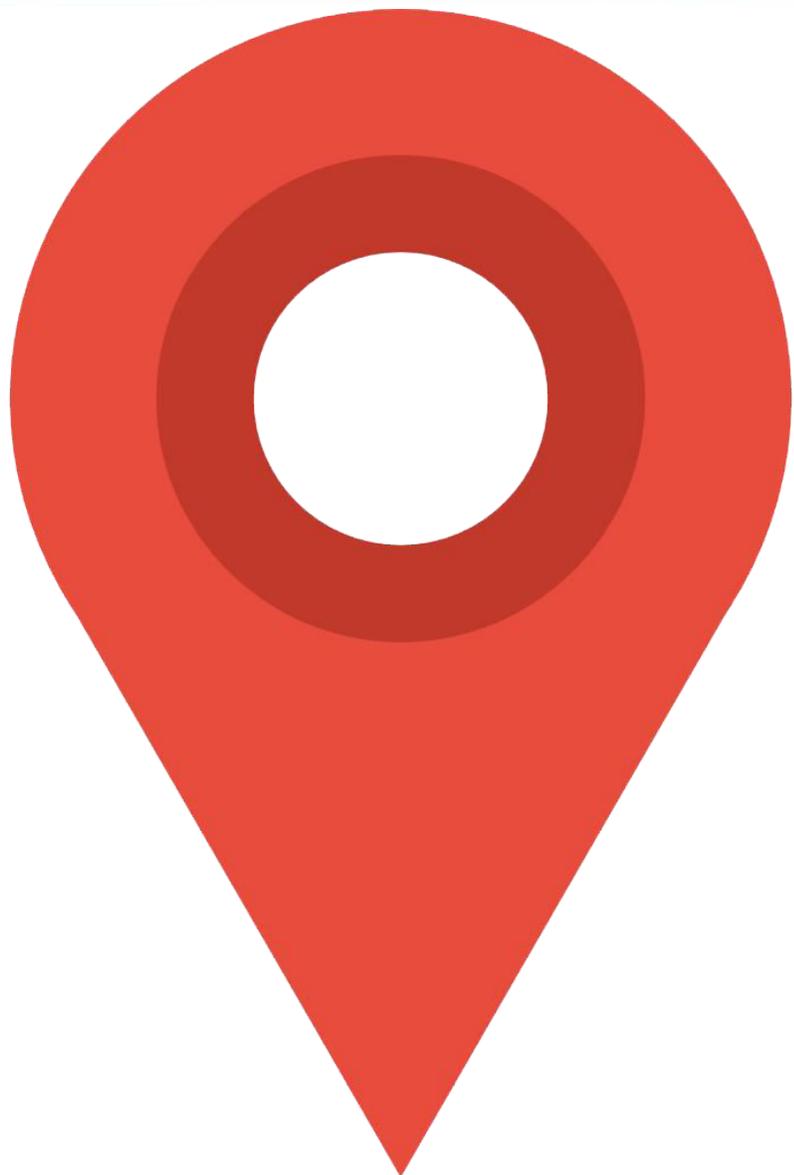


## Motivo 5: Com tijolão, ninguém sabe onde você está



# Motivo 5: Com tijolão, ninguém sabe onde você está





Google



## Histórico de localização

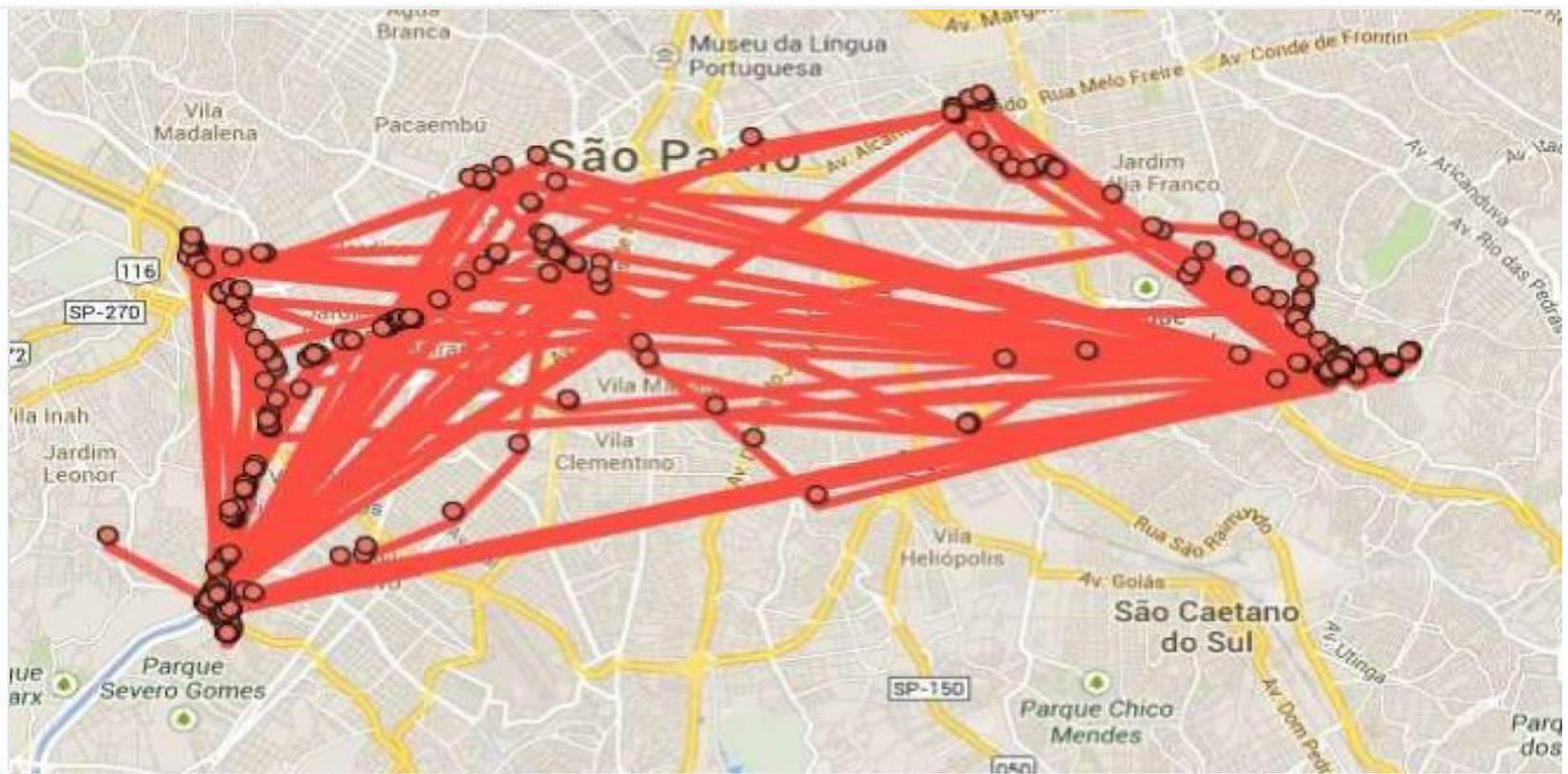


Mostrar: 30 dias

Localização	Tempo	Atividade
...	...	...
...	...	...
...	...	...
...	...	...

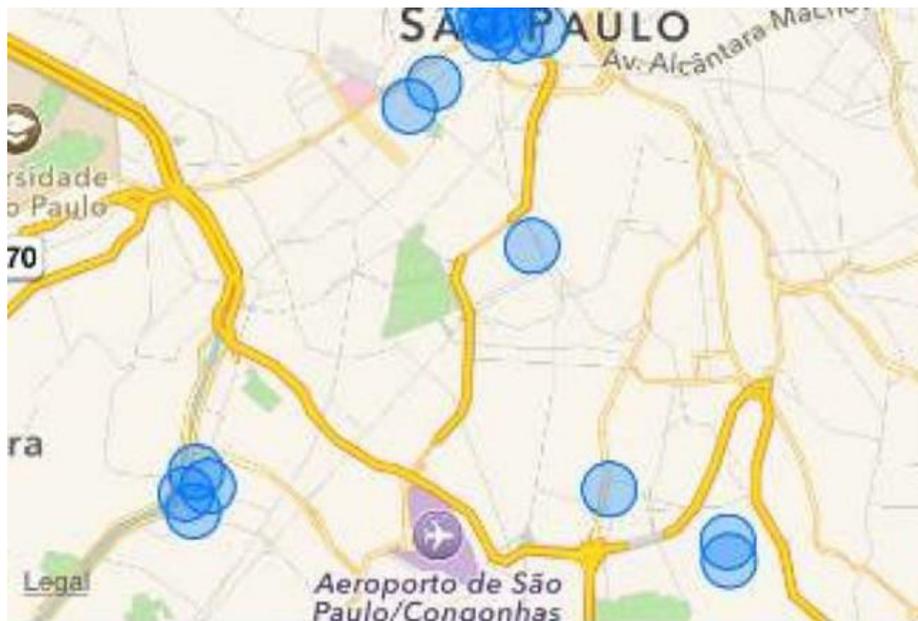
- ▶ Mostrar marca temporal
- Exportar para KML
- Excluir o histórico desse período
- Excluir todo histórico

Alguns pontos foram ocultados da visualização. [Mostrar todos os pontos](#) Saiba mais



Distância do local de partida (maior distância: 49,913 km)  
Passe o mouse sobre o gráfico para mostrar a localização no mapa





## Casa

55 visitas registradas desde

## Ponte Caio Pompeu De Toledo

44 visitas registradas desde

## Rua Amaral Gurgel, 314-392

25 visitas registradas desde

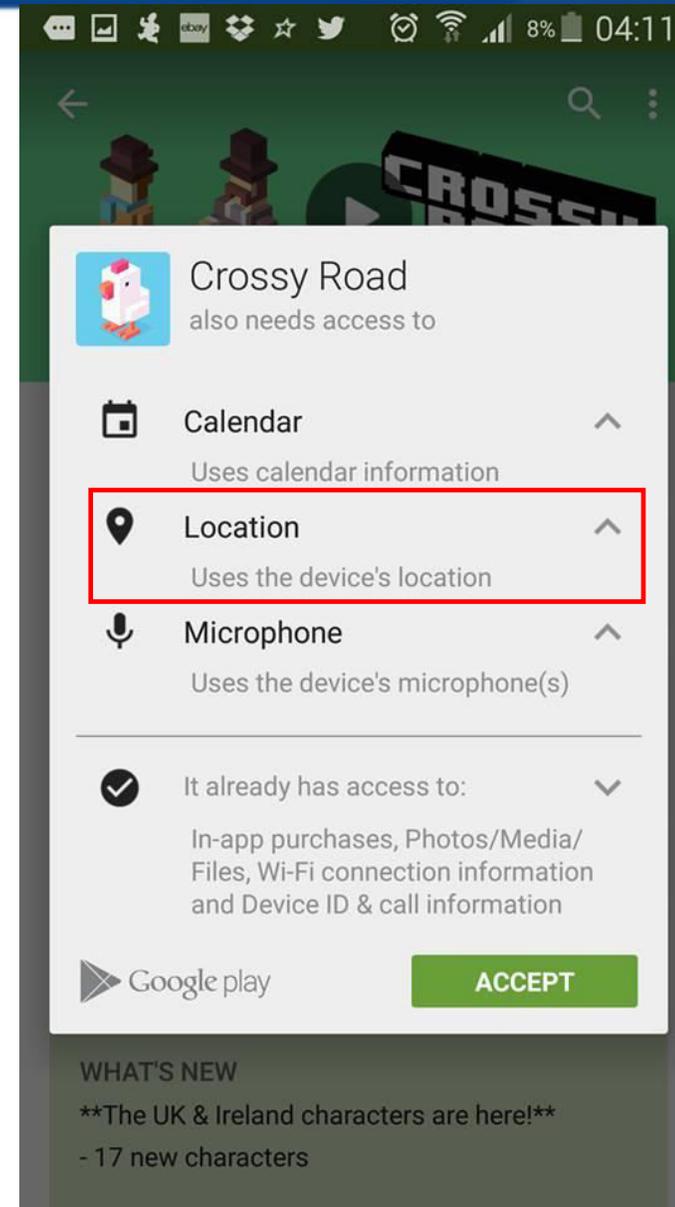
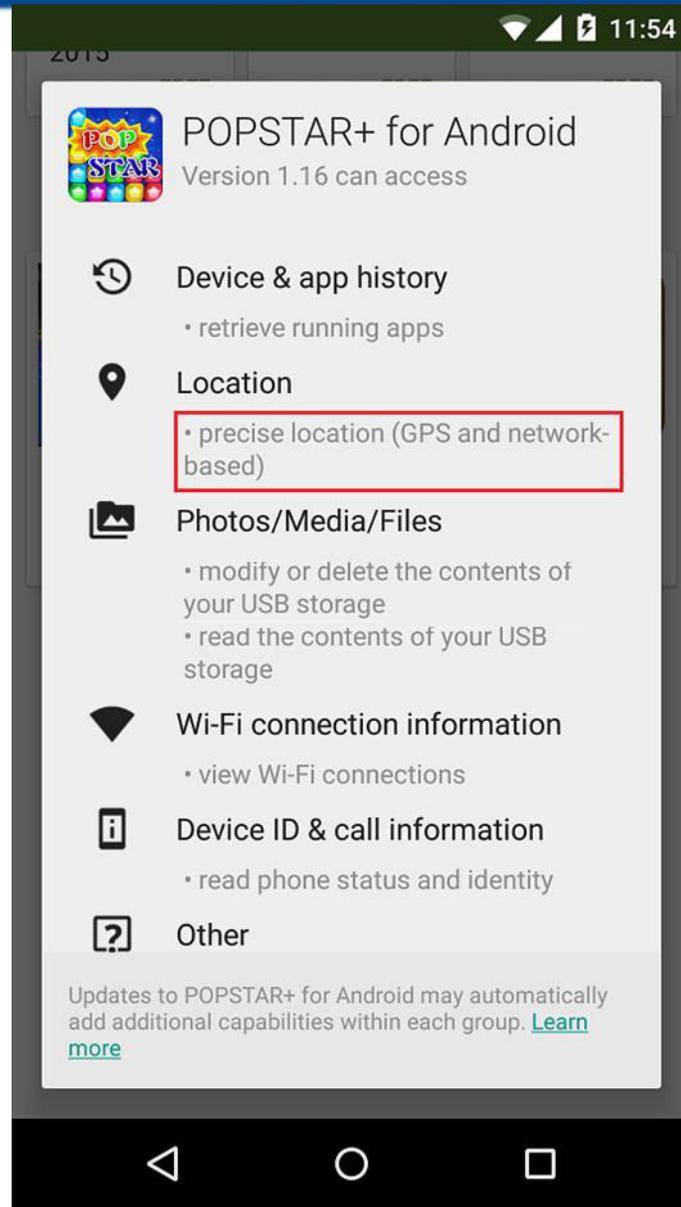
## Avenida Doutor Chueri Zaidan

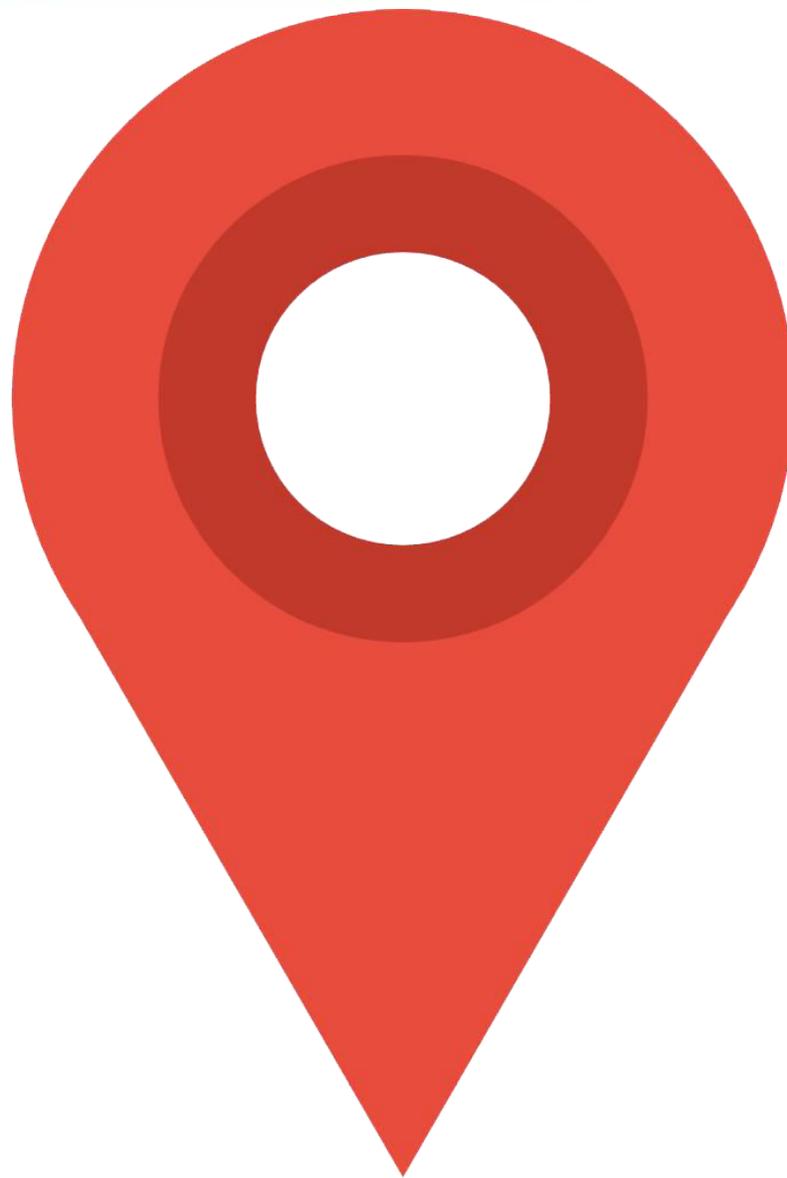
08:50 - 14:03

08:31 - 17:44

14:00 - 17:40

# Motivo 5: Com tijolo, ninguém sabe onde você está





-  **Check-in**
-  **Compartilhar fotos das redondezas da residência ou do caminho de rotina**
-  **Compartilhar fotos de local de trabalho**
-  **Postar planos de viagem pessoal/profissional**
-  **Postar informações de rotina pessoal (caminhos, lazer, companhias, etc.)**



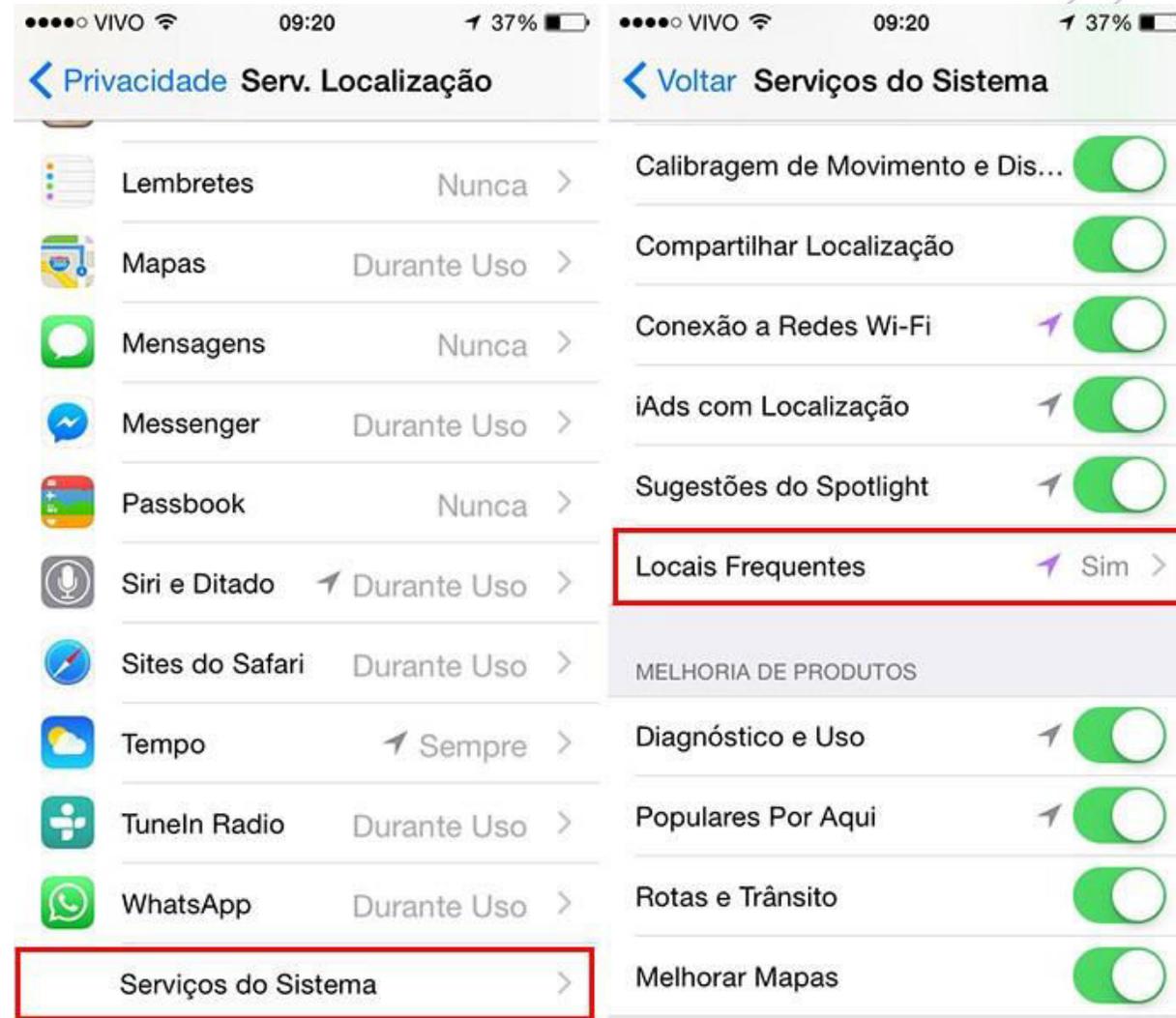
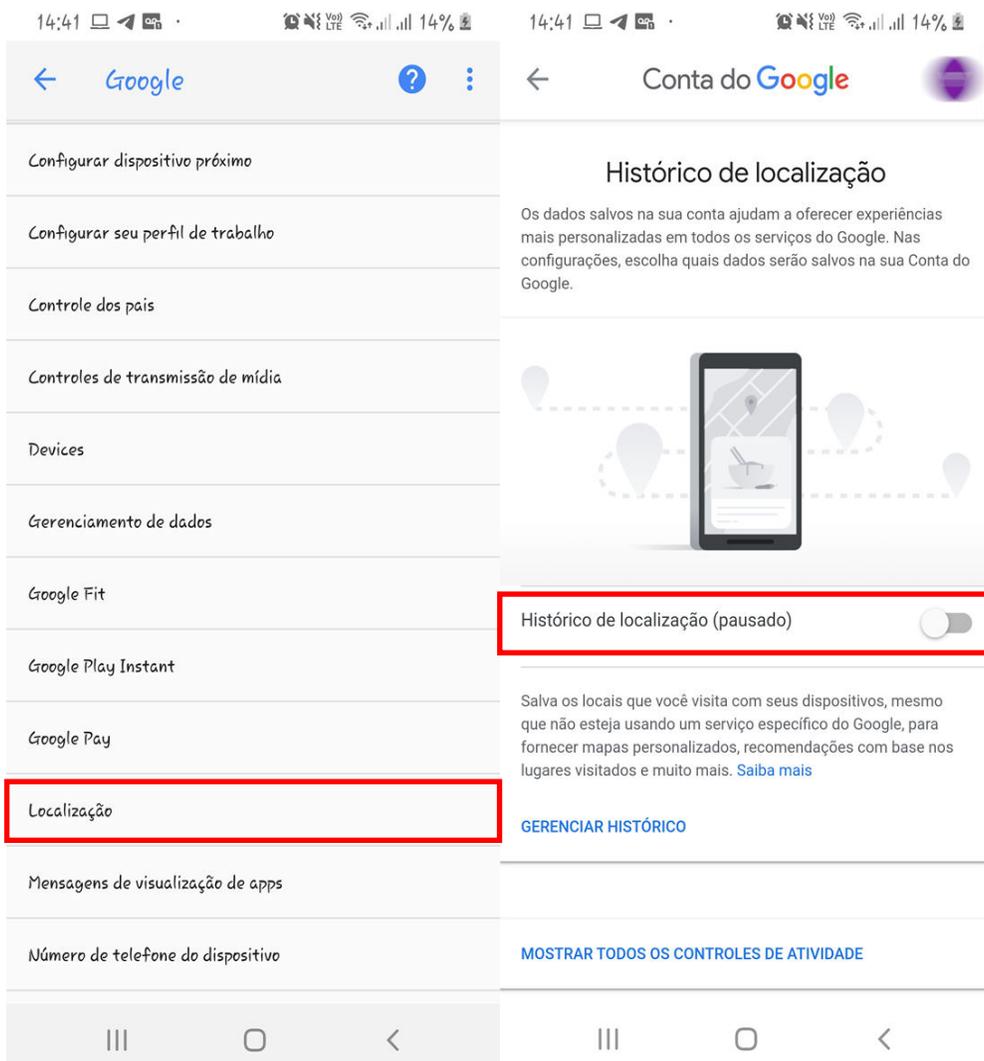
**VENDO**

TRATAR COM PAULO SILVA,  
CASADO COM ANA SILVA,  
TRABALHA NA HOTLINE S.A.,  
PAI DE ANTÔNIO E JÚLIA.

5588-4556 (À NOITE)  
ATÉ 21H, PORQUE CHEGO CANSADO  
DA ACADEMIA E DURMO CEDO.

**CUIDADO. VOCÊ PODE ESTAR  
AGINDO ASSIM NA INTERNET.**  
Privacidade é segurança. Proteja seus dados.

## Desativando o histórico de localização



# MOTIVO 6

## Tijolão não é hackeado







### Aplicativos maliciosos

Allow

Don't Allow

### Permissões desnecessárias e acesso não-autorizado a recursos



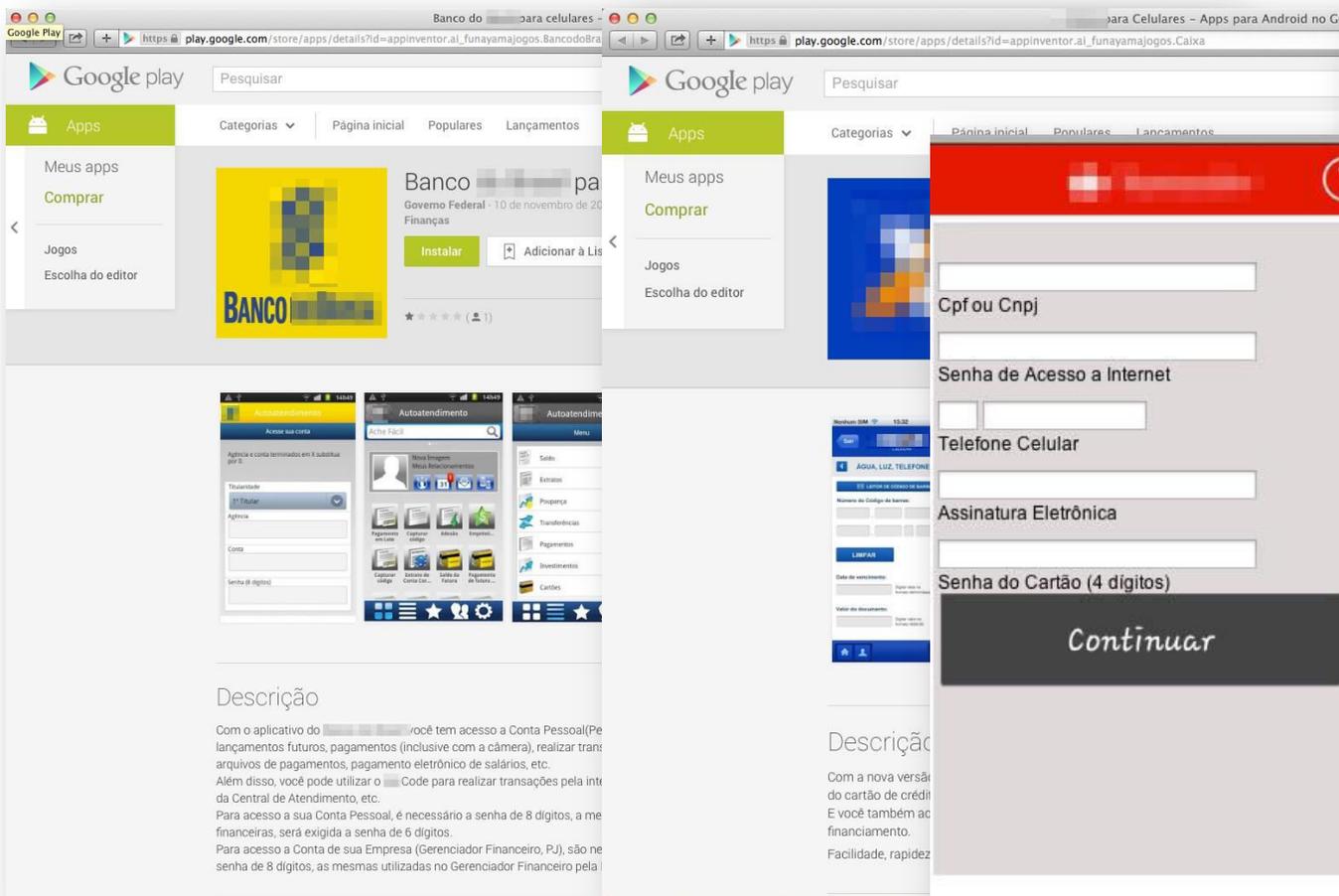
### Sim Swap



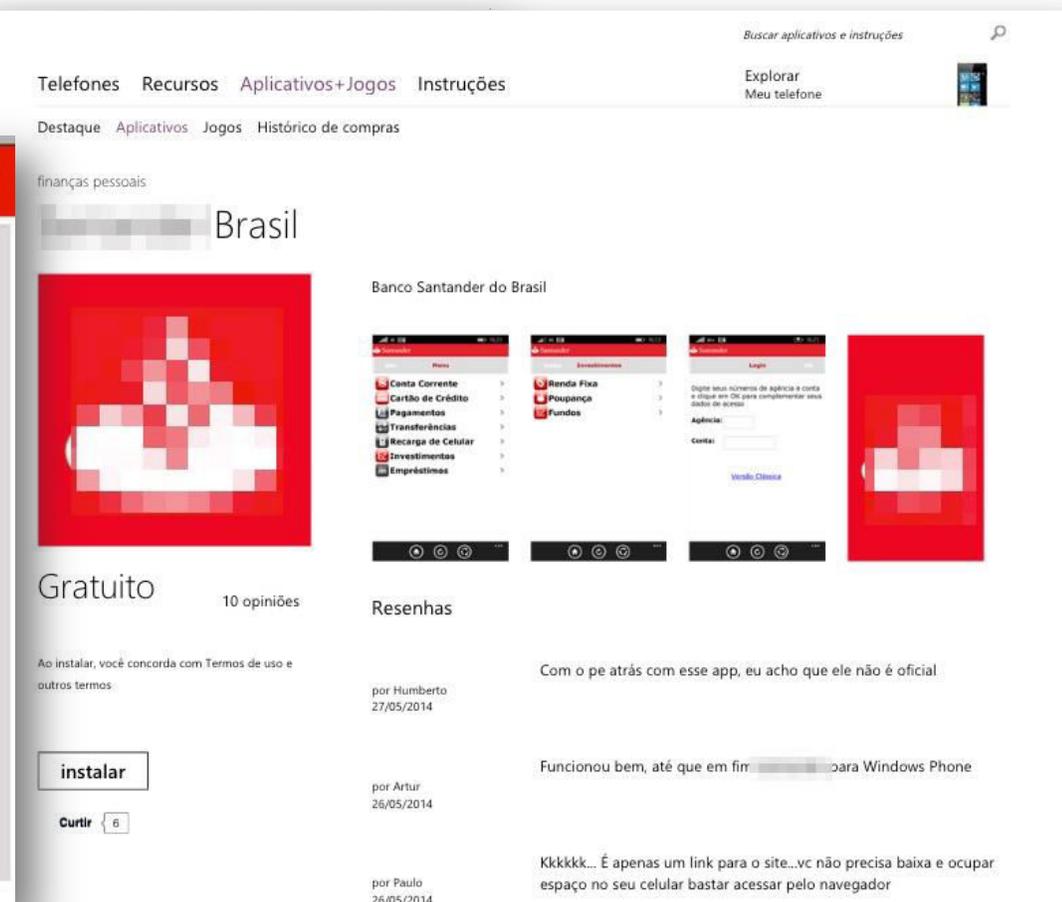
### Duplo fator de autenticação



## Aplicativos maliciosos



The screenshot shows the Google Play Store interface for an app named 'Banco do Tijolão'. The app is listed as being developed by 'Governo Federal' and has a rating of 1 star. The app icon is a yellow square with a pixelated pattern. Below the app listing, there are several screenshots of the app's interface, showing a login screen with fields for 'Cpf ou Cnpj', 'Senha de Acesso a Internet', 'Telefone Celular', 'Assinatura Eletrônica', and 'Senha do Cartão (4 dígitos)'. A large red button labeled 'Continuar' is visible at the bottom of the app preview. The description of the app is partially visible, mentioning access to a personal account and various services.



This screenshot shows the app's page on the Google Play Store. The app is titled 'Brasil' and is listed as 'Gratuito' (Free) with '10 opiniões' (10 reviews). The 'instalar' (Install) button is prominent. Below the app icon, there are several user reviews. One review from Humberto (27/05/2014) states: 'Com o pe atrás com esse app, eu acho que ele não é oficial'. Another review from Artur (26/05/2014) says: 'Funcionou bem, até que em fir... para Windows Phone'. A review from Paulo (26/05/2014) says: 'Kkkkk... É apenas um link para o site...vc não precisa baixa e ocupar espaço no seu celular bastar acessar pelo navegador'. The app's description is partially visible, mentioning 'finanças pessoais' and 'Banco Santander do Brasil'.



## Aplicativos maliciosos

Allow

Don't Allow

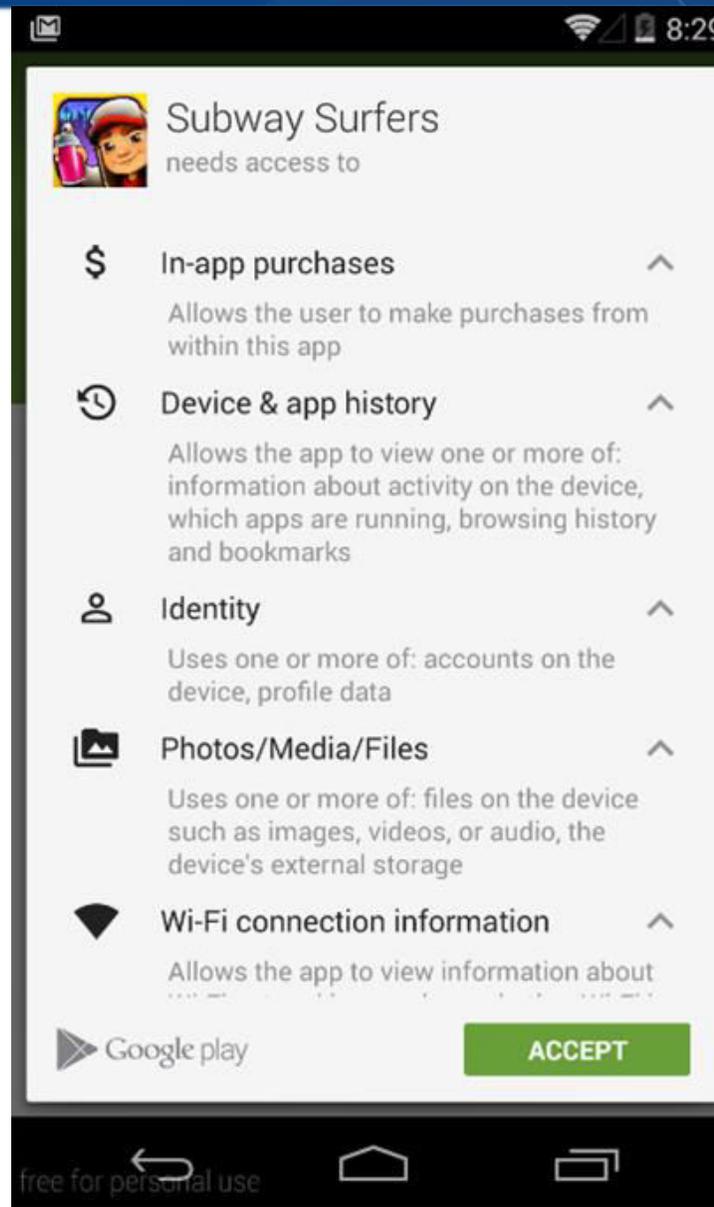
## Permissões desnecessárias e acesso não-autorizado a recursos



## Sim Swap



## Duplo fator de autenticação





## Aplicativos maliciosos

Allow

Don't Allow

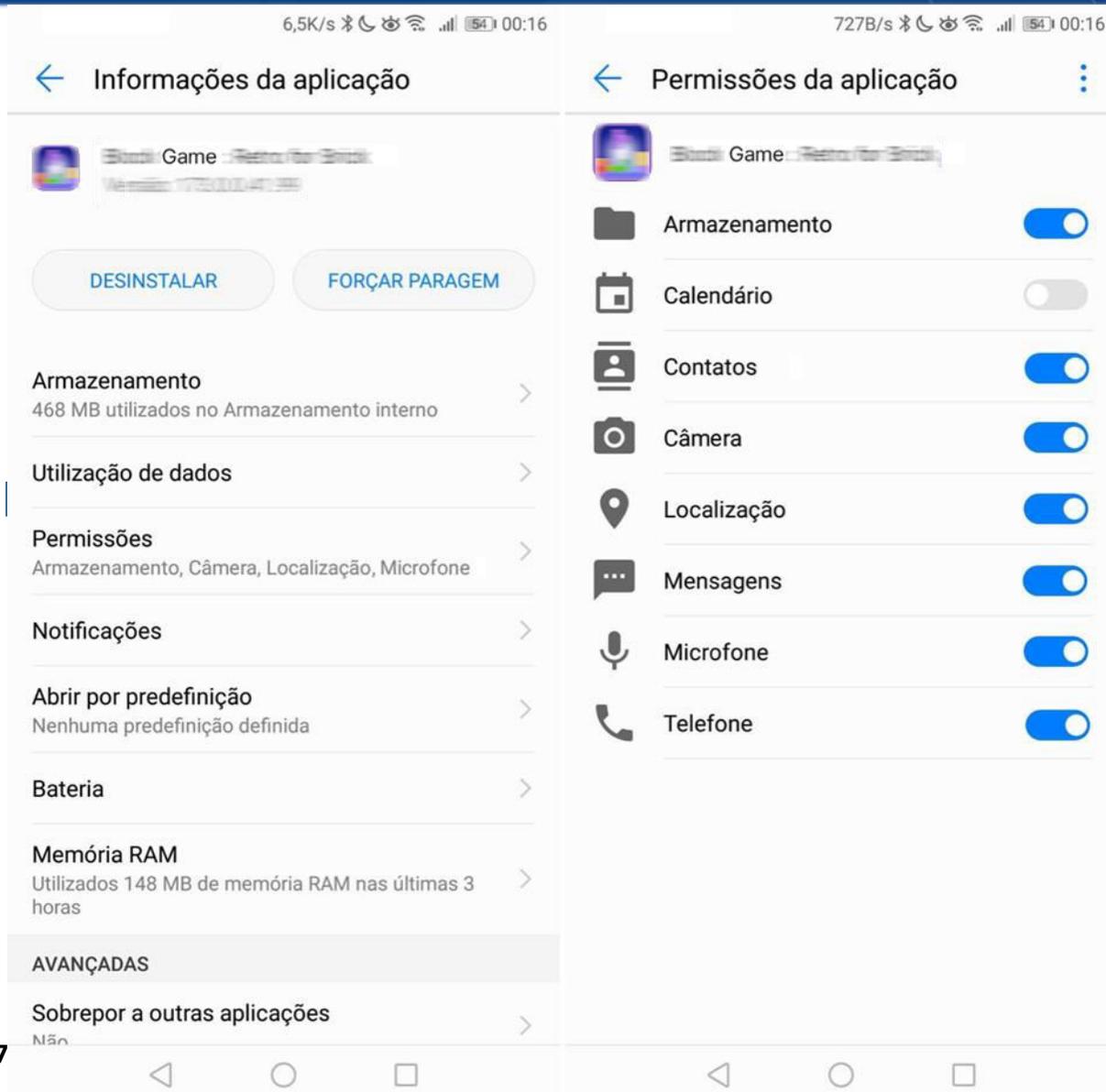
## Permissões desnecessárias e acesso não-autorizado a



## Sim Swap



## Duplo fator de autenticação



# MOTIVO 7

**Tijolão tem jogo da cobrinha.**





# VOLTANDO AO MOTIVO 6

## Tijolão não é hackeado



## Google admite ouvir gravações captadas por assistente virtual

Empresa alega que áudios são usados para melhorar a compreensão de línguas e sotaques

AFP

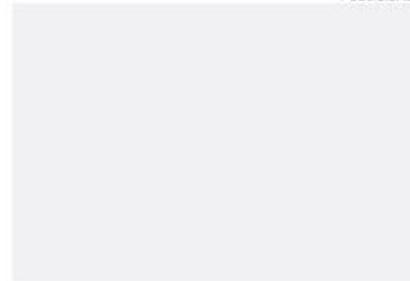
12/07/2019 - 11:18 / Atualizado em 12/07/2019 - 11:27



O Google Assistente funciona em smartphones Android e alto-falantes inteligentes Foto: Justin Sullivan / AFP

MOUNTAIN VIEW — O **Google** admitiu na quinta-feira que seus funcionários tiveram acesso a gravações realizadas por seu **assistente virtual**, após revelações do canal público belga **VRT**.

PUBLICIDADE



## Mensagens íntimas

Mas que tipo de buscas ou conversas chegam a esses transcritores? Tudo o que é dito no celular, desde mensagens de texto até conversas familiares, entre amigos, discussões e até papos íntimos de casais. A consulta de endereços e de lugares ou lojas, [bem como mensagens de sexo e a privacidade dos usuários](#) é posta em xeque, pois nos áudios se escutam dados sensíveis em um ambiente que o Google não controla por completo.

Nos casos de áudios pertencentes a interações com o Google Home, a ativação do sistema também é feita pelo 'Ok Google'. Várias vezes, entretanto, a gravação começa sem esse aviso. "Acontece muito que a gravação começa sem esse aviso. Acontece muito que a pessoa diz algo parecido e ativa o microfone. Isso acontece com as conversas pessoais sem saber que foi ativado", dizem os transcritores. Nessas gravações, o que se escuta é a conversa pessoal, mas outros continuam com sua conversa pessoal sem saber que foi ativado", dizem os transcritores. É apagar a luz, colocar música, abrir a garagem, ligar o ar condicionado...

A primeira fissura — conhecida — na couraça que custodia os dados pessoais que os usuários enviam ao Google ocorreu com o vazamento de mil dessas gravações ao canal de televisão belga VRT NWS. Isso provocou o

A photograph of Mark Zuckerberg sitting at a table with a young boy. Zuckerberg is wearing a grey t-shirt and looking towards the boy. The boy is wearing a blue shirt and looking back at Zuckerberg. The background is slightly blurred, showing other people in a public setting.

**MY DAD SAYS  
YOU'RE SPYING  
ON US**

**HE'S NOT  
YOUR DAD**



Aplicativos maliciosos

Ativa  
De 0 a 100

Permissões desnecessárias  
e acesso não-autorizado a recursos



Sim Swap



Duplo fator de autenticação

Como funciona a fraude (1)





## Aplicativos maliciosos



## Permissões desnecessárias e acesso não-autorizado a recursos



## Sim Swap



## Duplo fator de autenticação

## Como funciona a fraude (2)





Aplicativos maliciosos

Ativa  
De 0 a 100

Permissões desnecessárias  
e acesso não-autorizado a recu

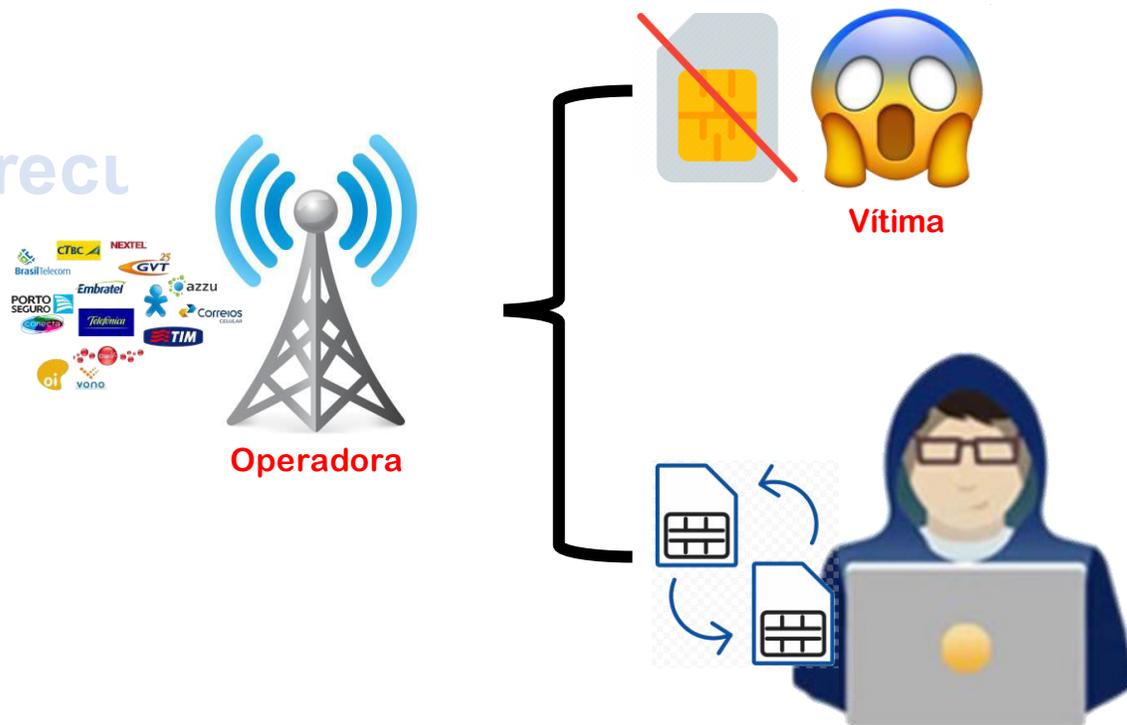


Sim Swap



Duplo fator de autenticação

## Como funciona a fraude (3)





## Aplicativos maliciosos



## Permissões desnecessárias e acesso não-autorizado a recursos

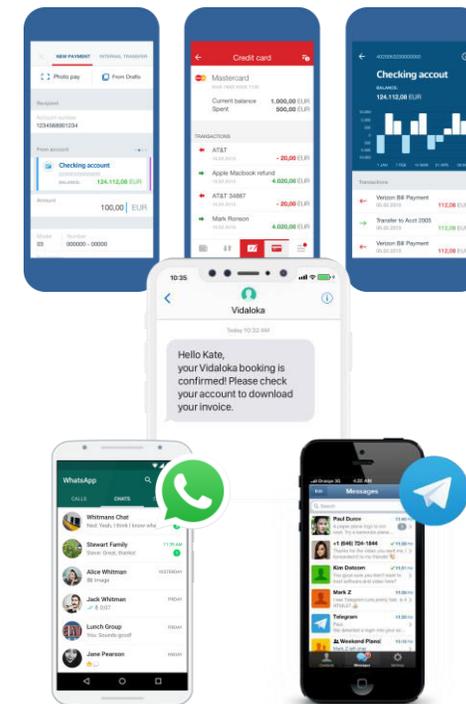
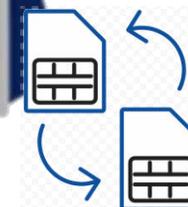


## Sim Swap



## Duplo fator de autenticação

## Como funciona a fraude (4)





## Aplicativos maliciosos

Ata  
Do C.Alex

Permissões desnecessárias  
e acesso não-autorizado a recursos



Sim Swap



Duplo fator de autenticação





Aplicativos maliciosos



Permissões desnecessárias e acesso não-autorizado a recursos



Sim Swap



Duplo fator de autenticação

## Alguns softwares de 2FA



Google Authenticator



Duo



Microsoft Authenticator



Authy



FreeOTP



LastPass



andOTP

etc.

# MOTIVO 8

**Tijolão não tem falha crítica de segurança de software.**

## Falha de s vulneráveis

Vulnerabilida

Por Redação | 04/09/2018



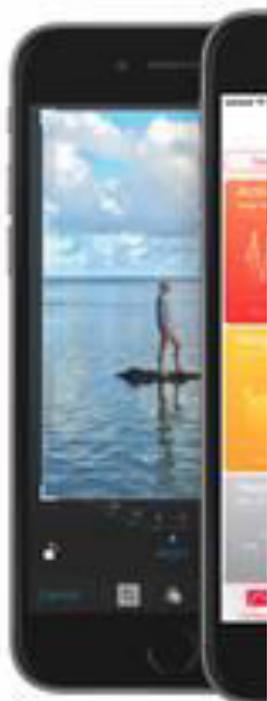
Crédito: andrey\_pogov/Sh

A Check Point Res  
revelar uma falha  
Samsung, Huawei

## iOS tem f facilmente



Por Paulo Higa  
4 anos atrás



Uma falha de seguran  
intencionadas rouben  
pelo menos desde jan

Home > Produtos > Smartphone

# Vários smartphones Android já vêm com vulnerabilidades de fábrica

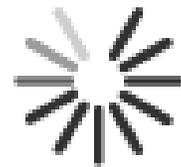
Por Patrícia Gnipper | 10 de Agosto de 2018 às 21h55

Pesquisadores da empresa de segurança Kryptowire encontraram falhas de segurança em aparelhos com Android, falhas essas que já vêm de fábrica. O motivo são as personalizações que as fabricantes fazem no Android para seus diferentes aparelhos, sendo que [Asus](#), [Essential](#), [LG](#) e [ZTE](#) já prometeram corrigir essas vulnerabilidades encontradas.

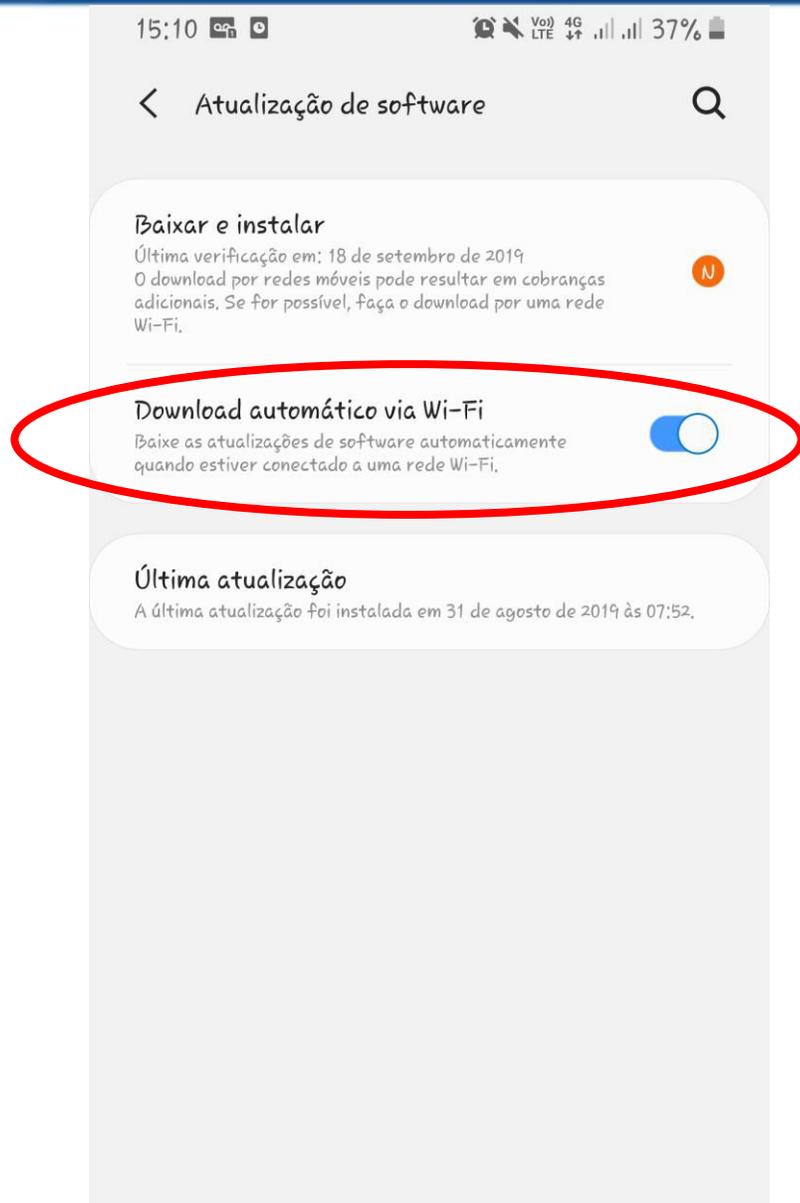
Bugs no firmware de 10 dispositivos foram detectados pela empresa em questão, sendo que essas falhas podem permitir que um invasor faça de tudo um pouco: desde travar o dispositivo e impedir que o usuário o desbloqueie, passando pelo controle de câmeras e microfones, a até mesmo instalar aplicativos maliciosos sem que o usuário perceba.

Segundo a Kryptowire, tais falhas não são nativas do Android: elas surgem após as fabricantes ajustarem o código do sistema para modificá-lo de acordo com suas preferências. Contudo, ano a ano vemos este cenário se repetir, o que pega mal para a

Atualizando software...



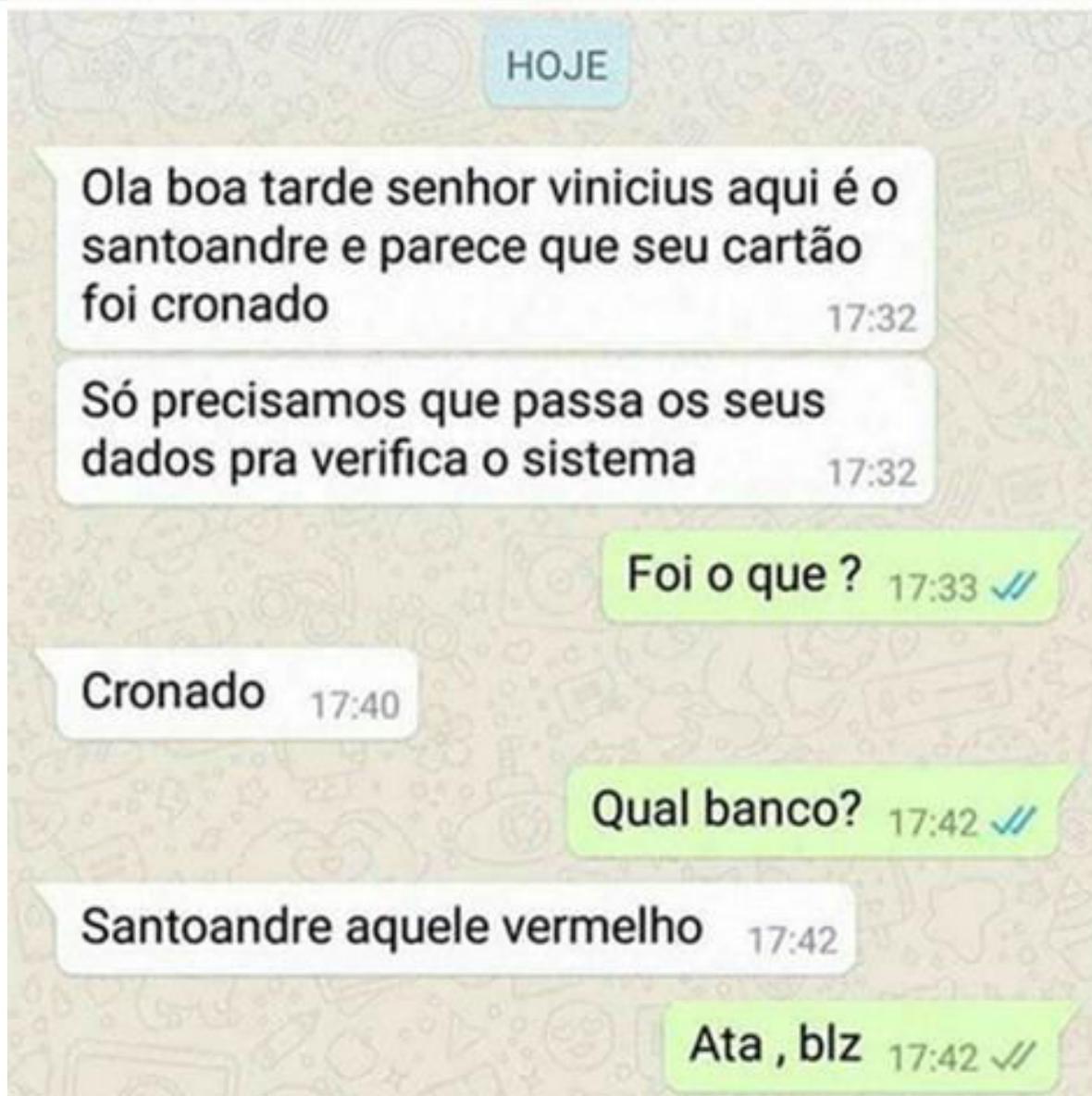
## Motivo 8: Tijolão não tem falha crítica de segurança de software



# MOTIVO 9

**Tijolão não cai em phishing/smshing.**





Mensagem  
Hoje, 17:16

Prezado Cliente regularize agora o seu dispositivo e evite o bloqueio de suas senhas, acesse [www.santanderbr.com.br](http://www.santanderbr.com.br) ou procure sua agencia.

27880 ▾ CHAMAR

SMS/MMS

domingo, 12 de março de 2017

BB INFORMA: para continuar usando sua conta e preciso a liberacao de seu smartfone, acesse <http://acesso-bb-seguranca.com/bb> e libere agora.

12:4



Mensagem  
Hoje, 19:19

SANTANDER: Compra aprovada as 19:18:54, Para ver seu comprovante ou efetuar o cancelamento, Acesse:

Toque para carregar a pré-visualização

goo.gl



Text Message  
Today, 11:07

Oi [REDACTED], seu Cartao Caixa 5536 XXXX XXXX 7760 vence em 02/19. Acesse <https://atualize.digital/cartoes.caixa/6cc756> e atualize seu cadastro.

Oi [REDACTED], seu Cartao Caixa 5536 XXXX XXXX 6400 vence em 02/19. Acesse <https://atualize.digital/cartoes.caixa/a42421> e atualize seu cadastro.

Oi [REDACTED], seu Cartao Caixa 5536 XXXX XXXX 4031 vence em 02/19. Acesse <https://atualize.digital/cartoes.caixa/bf2c56> e atualize seu cadastro.

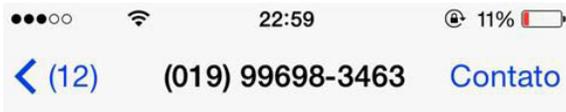
Oi [REDACTED], seu Cartao Caixa 5536 XXXX XXXX 9560 vence em 02/19. Acesse <https://atualize.digital/cartoes.caixa/4eccea> e atualize seu cadastro.

Text Message  
Today 01:15

Dear Customer,

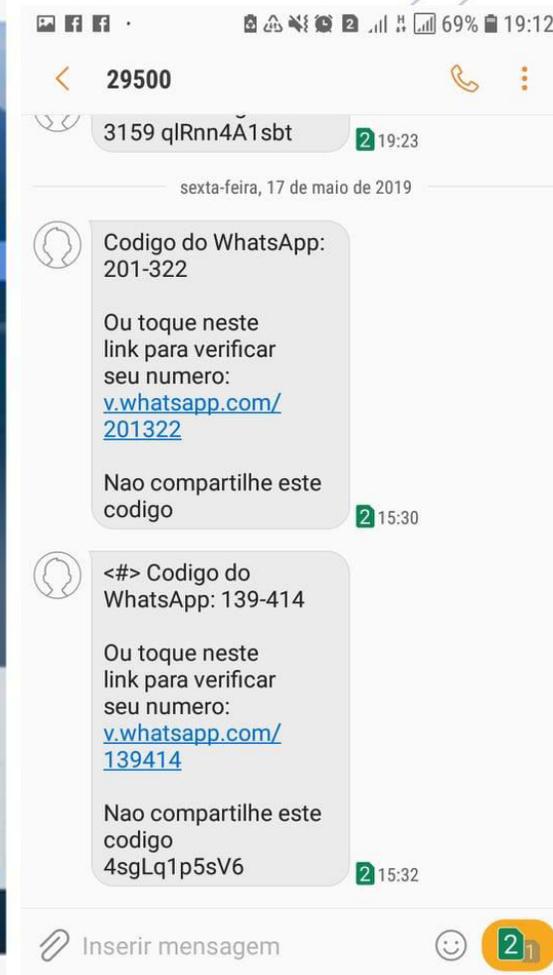
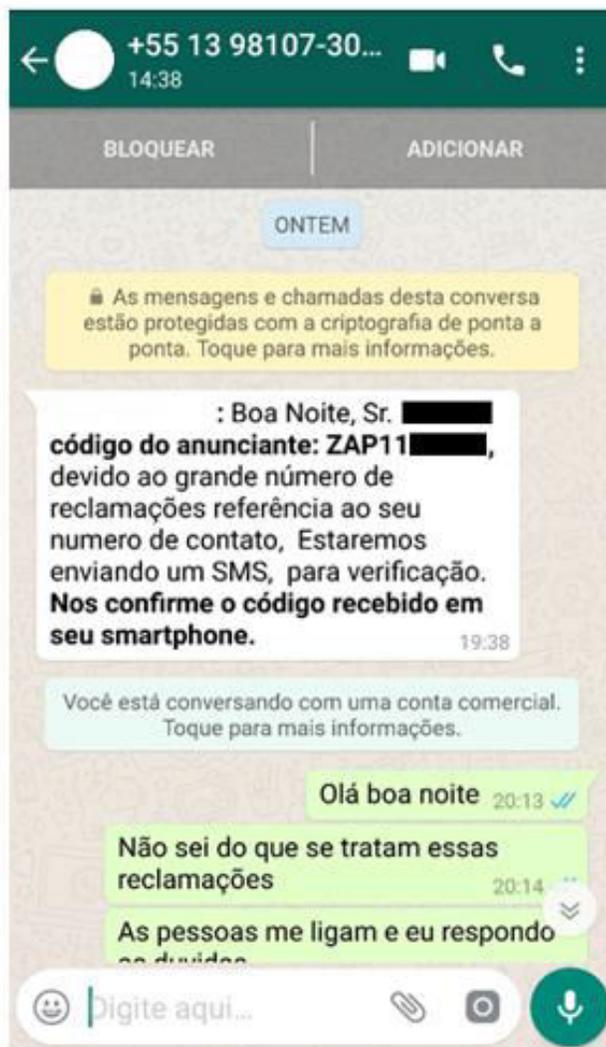
Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.

Apple smsSTOPto43420



Mens. de Texto  
Hoje 21:04

Apple informa  
Seu dispositivo iPhone em modo perdido foi localizado acesse <http://www.i-cloud.hol.es> para obter mais informações.





# MOTIVO 10

**Tijolão não tem gemidão do whatsapp.**



**Obrigado!**

**Yuri Alexandro**

**cais@cais.rnp.br**



MINISTÉRIO DA  
DEFESA

MINISTÉRIO DA  
CIDADANIA

MINISTÉRIO DA  
SAÚDE

MINISTÉRIO DA  
EDUCAÇÃO

MINISTÉRIO DA  
CIÊNCIA, TECNOLOGIA,  
INOVAÇÕES E COMUNICAÇÕES

