WORKSHOP DE CIBERSEGURANÇA

PROTEÇÃO DE DADOS EM TEMPOS DE COVID-19

Boas práticas e medidas técnicas para proteção dos dados pessoais *online*

Marcelo Caiado

Chefe da Assessoria Nacional de Perícias de TIC

Analista do MPU / Perícia / TIC

23 de novembro de 2020

OEA Mais direitos para mais pessoas

ITS Instituto de Tecnologia & Sociedade do Rio

GREAT for PARTNERSHIP

MPF Ministério Público Federal

Todas as opiniões aqui apresentadas são exclusivas do palestrante, apenas de caráter ilustrativo e não possuem nenhum vínculo com o MPF ou qualquer outro órgão ou instituição

Apresentação

- *Graduado em Processamento de Dados (UCB) e em Administração de Sistemas de Informações (UNEB)*
- *Especialista em Gestão Pública (FGV)*
- *Mestre em Ciência da Computação (UnB)*
- *Analista do MPU / Perícia / TIC (1997)*
- *CyberForensics Analyst / Blackberry – 2008 a 2010*
- *Mantenedor do site http://dfir.com.br*

“Tecnologia Disruptiva: Designação atribuída a uma inovação tecnológica (produto ou serviço) capaz de derrubar uma tecnologia já preestabelecida no mercado.”

Fonte: https://www.dicio.com.br/disruptivo/

“No momento, nós estamos em um interregno. Um interregno que significa, simplesmente, que a antiga maneira de agir não funciona mais, e novos modos de agir ainda não foram inventados. Esse é o interregno.”

Com quem estamos lidando?

Crime organizado, insiders, nações, hacktivistas/terroristas, oportunistas

https://coronavirus.jhu.edu/map.html

JOHNS HOPKINS UNIVERSITY & MEDICINE | CORONAVIRUS RESOURCE CENTER

Home | Tracking | Testing | Tracing | Vaccines | By Region | News & Resources | About

Tracking Home | Critical Trends | Global Map | U.S. Map | Data in Motion

COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

Global Cases
6,071,401

Cases by Country/Region /Sovereignty

- 12,249,198 US
- 9,139,865 India
- 6,071,401 Brazil
- 2,191,180 France
- 2,096,749 Russia
- 1,556,730 Spain
- 1,515,802 United Kingdom
- 1,408,868 Italy
- 1,370,366 Argentina
- 1,248,417 Colombia

Admin0 | Admin1 | Admin2

Last Updated at (M/D/YYYY)
11/23/2020, 7:25 AM

Cumulative Cases | Active Cases | Incidence Rate | Case-Fatality Ratio | Testing Rate

191
countries/regions

Lancet Inf Dis Article: Here. Mobile Version: Here. Data sources: Full list. Downloadable database: GitHub, Feature Layer.
Lead by JHU CSSE. Technical Support: Esri Living Atlas team and JHU APL. Financial Support:

Global Deaths
169,183

169,183 deaths
Brazil

Global Deaths

US State Level
Deaths, Recovered

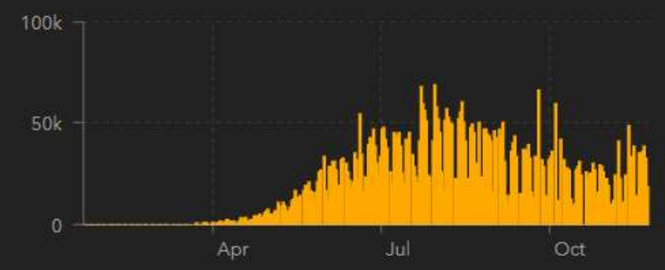
34,319 deaths, 83,307 recovered
New York US

21,013 deaths, 913,796 recovered
Texas US

18,727 deaths, recovered
California US

17,991 deaths, recovered
Florida US

US Deaths, Recov...



Daily Cases

Security Holes Opened Back Door To TCL Android Smart TVs

November 12, 2020 09:20 by Paul Roberts

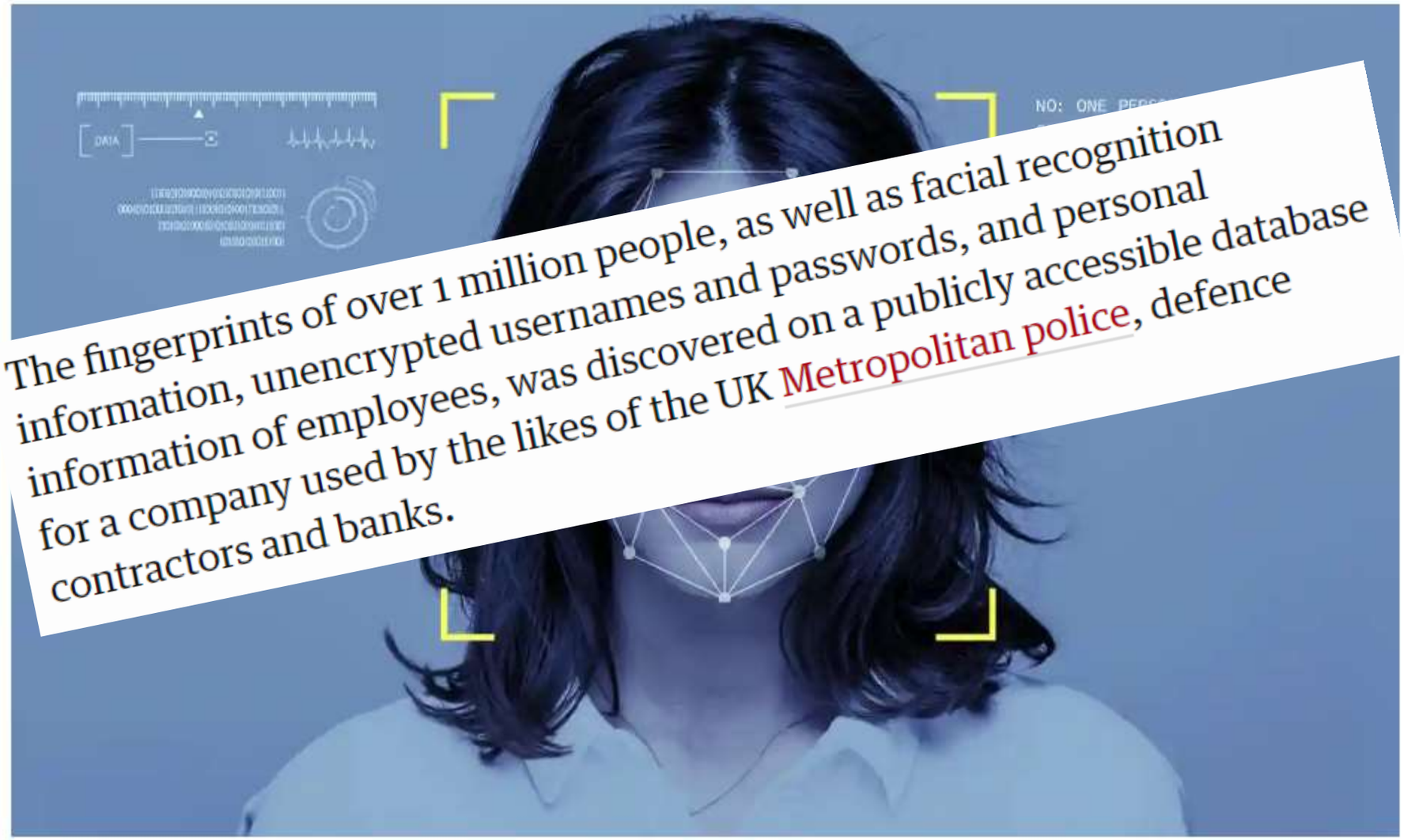
Millions of Android smart television sets from the Chinese vendor **TCL Technology Group Corporation** contained gaping software security holes that researchers say could have allowed remote attackers to take control of the devices, steal data or even control cameras and microphones to surveil the set's owners.

The security holes appear to have been patched by the manufacturer in early November. However the manner in which the holes were closed is raising further alarm among the researchers about whether the China-based firm is able to access and control deployed television sets without the owner's knowledge or permission.

Major breach found in biometrics system used by banks, UK police and defence firms

Wed 14 Aug 2019 08.11 BST

Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database



The fingerprints of over 1 million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees, was discovered on a publicly accessible database for a company used by the likes of the UK Metropolitan police, defence contractors and banks.

▲ Security company Suprema uses facial recognition, fingerprints and passwords to secure facilities for the likes of the Metropolitan Police, defence contractors and banks. Photograph: izusek/Getty Images/iStockphoto

https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

Zoom security issues: Here's everything that's gone wrong (so far)

By Paul Wagenseil 5 days ago

More than a dozen security and privacy problems have been found in Zoom. Here's an updated list.

Comments (8)

(Image credit: Rido/Shutterstock)

Are you using Zoom? Everyone who's had to work, or do schoolwork, from home during the coronavirus lockdown seems to be using the video-conferencing platform for meetings, classes and even social gatherings.

There are good reasons Zoom has taken off and other platforms haven't. Zoom is easy to set up, easy to use, lets up to 100 people join a meeting for free and now even generates live captions. It just works.

The latest: Monday, Nov. 16: Zoom finally busts Zoom-bombing

One of the biggest problems with Zoom has been "Zoom bombing," in which uninvited participants crash a Zoom meeting and disrupt it. Over the weekend, Zoom released two new features to combat this.

One, "Suspend Participant Activities," lets the meeting host pause the meeting, kick out disruptive participants, and then resume the meeting. The other, "Report by Participants," extends to meeting participants the ability to report disruptive participants, a remedy that previously had been given only to meeting hosts.

Tuesday, Nov. 10: FTC says Zoom lied about security

The Federal Trade Commission announced that Zoom "misled users" and "engaged in a series of deceptive and unfair practices" regarding its own security. The FTC cited the fake end-to-end encryption uncovered in March and software that Zoom installed on Macs without authorization in 2018 and 2019.

Zoom must agree to yearly internal security reviews and external security reviews every other year and must implement a vulnerability-management program. Another stipulation was that Zoom offer customers multi-factor authentication, which it has already implemented.

Friday, Nov. 6: Zoom keystroke snooping

Researchers in Texas and Oklahoma discovered that it's possible to tell what someone is typing during a Zoom call just by watching their shoulders and arms.

Using a computer, the research team was able to figure out people's passwords up to 75% of the time, depending on camera resolution and whether the subject was wearing a sleeved shirt or had long hair.

Any kind of video-conferencing platform could be used for this, the researchers said, as could YouTube videos or streaming platforms like Twitch.

https://www.tomsguide.com/news/zoom-security-privacy-woes

The massive ransomware bill faced by Merck echoes the financial hits taken by other enterprises like Maersk and FedEx.

The full financial impact of the NotPetya ransomware campaign is still being tallied and, for pharmaceutical giant Merck, things don't look good. According to the firm's Friday earnings call, the attack cost them more than $300 million in Q3 alone, and is on track to hit that amount again in Q4 as well.

On the call, Merck CFO Robert Davis said that NotPetya had "negatively impacted third-quarter results, including an unfavorable revenue impact of approximately $135 million from lost sales and approximately $175 million in costs, spread across the cost of goods sold and the operating expense lines. We anticipate a similar impact to revenue and expenses in the fourth quarter, which is reflected in our updated guidance."

Due to a production shutdown caused by the attack, Merck saw sales reductions of around $240 million. This was because of "borrowing from the U.S. Centers for Disease Control and Prevention

https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/

Cuidado com suas mídias sociais

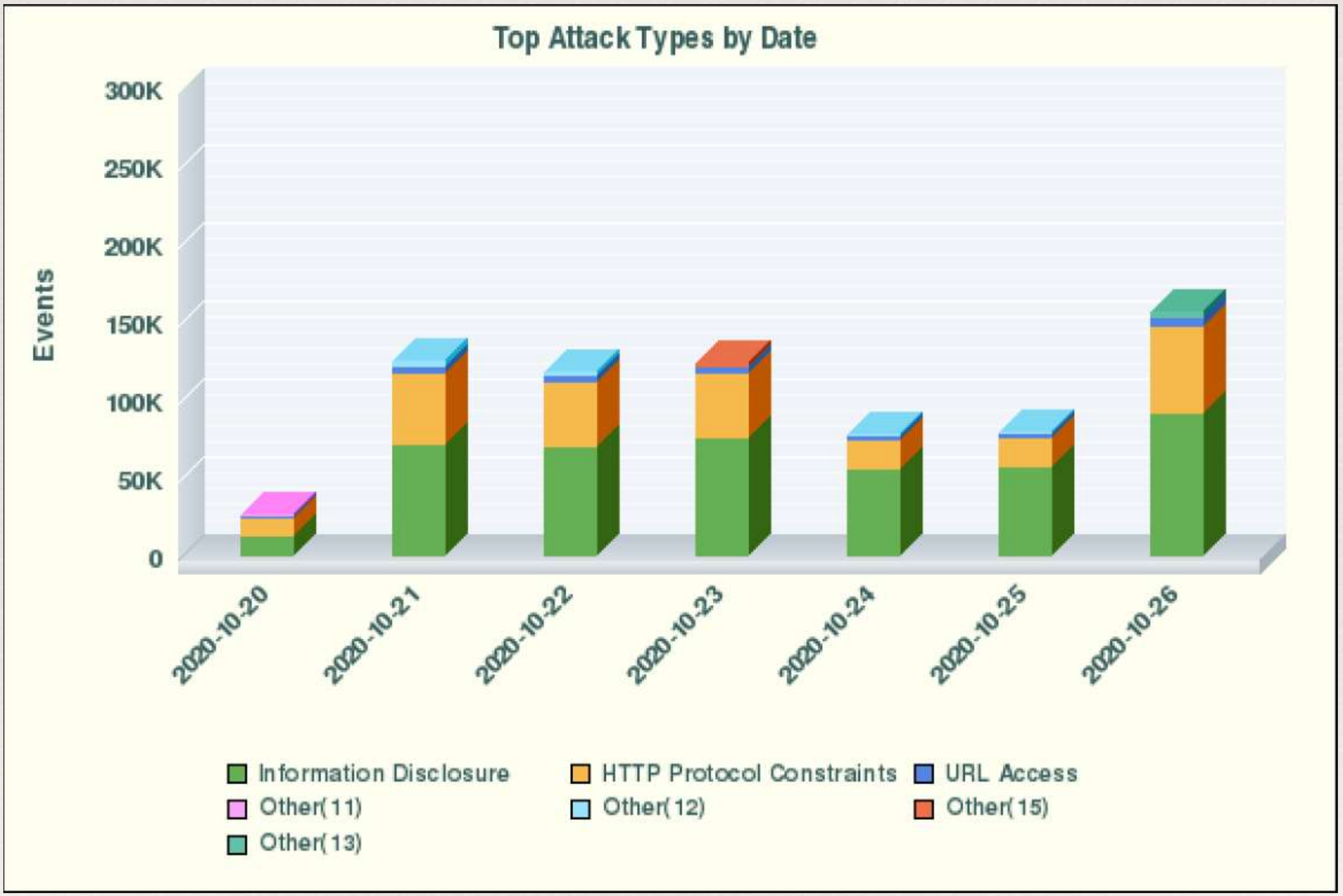
Jornal de Brasília

Vaticano investiga após conta do Papa no Instagram curtir foto de mode

CIDADES · POLÍTICA & PODER · ENTRETENIMENTO · BRASIL · ECONOMIA · MUNDO · TORCIDA

O Vaticano inciou uma investigação para apurar a curtida que a conta oficial do Papa Francisco deu numa foto sexy da modelo brasileira Natalia Garibotto, popularmente conhecida como Nata Gata.

A informação foi divulgada pela Catholic News Agency (CNA), que disse ter recebido o a informação de fontes dentro do próprio Vaticano. Segundo elas, as contas nas mídias sociais do chefe da Igreja Católica não são administradas pelo Papa, e sim por vários funcionários da Santa Sé. Uma investigação está em andamento para determinar quem está por trás do "like".



Proteja-se!

Google Authenticator

Google LLC Tools

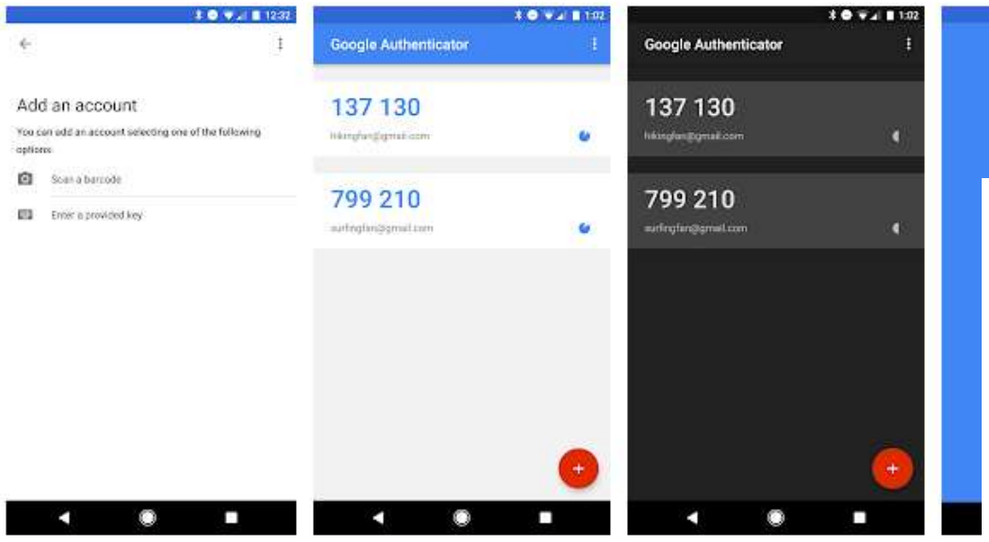
★★★★☆ 192,872

Everyone

This app is compatible with all of your devices.

You can share this with your family. Learn more about Family Library

Installed



Google Authenticator generates 2-Step Verification codes on your phone.

2-Step Verification provides stronger security for your Google Account by requiring a second verification when you sign in. In addition to your password, you'll also need a code generated Google Authenticator app on your phone.

Authy 2-Factor Authentication

Authy Tools

★★★★☆ 20,883

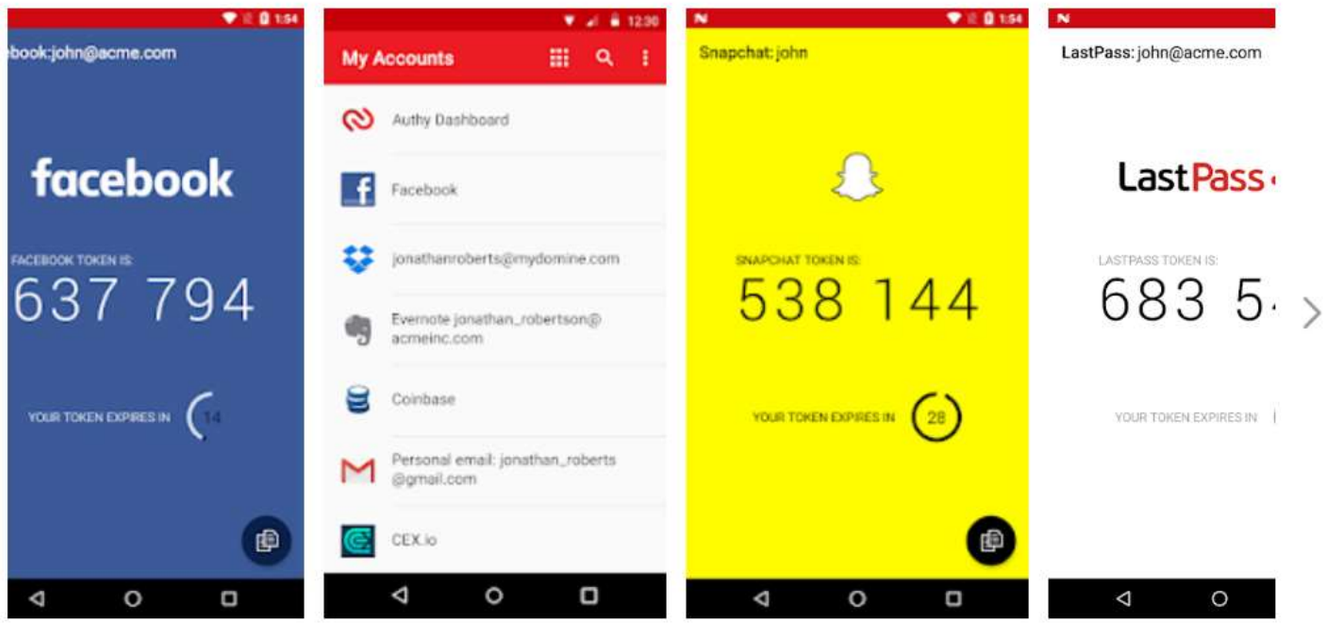
Everyone

This app is compatible with your device.

You can share this with your family. Learn more about Family Library

Add to Wishlist

Install



https://www.scoopwhoop.com/Heres-Why-You-Should-Just-Say-No-To-Pirated-Software/

0
/ 71

?

Community Score

No engines detected this file

4f2bdfa6a133148f60a91d0a83e51223fd5062ab37cd95082e9c8988a9416a7c

SpotifySetup.exe

871.32 KB
Size

2020-11-23 02:02:27 UTC
8 hours ago

EXE

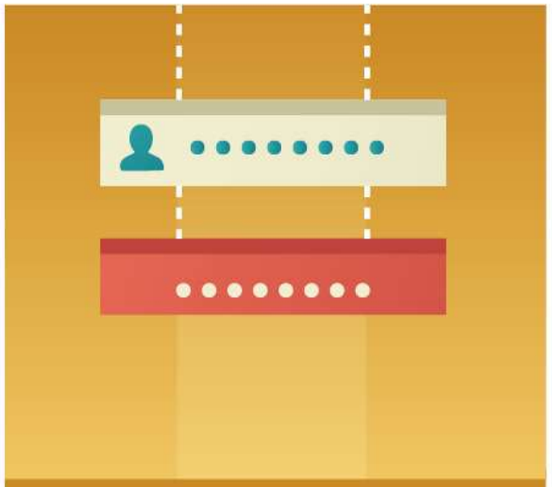
checks-network-adapters | direct-cpu-clock-access | invalid-rich-pe-linker-version | overlay | peexe | runtime-modules | signed

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	SecureAge APEX	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected
CMC	Undetected	Comodo	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected

https://www.virustotal.com

WHAT IS BUSINESS EMAIL COMPROMISE?



ILLEGAL ACCESS

Criminals gain entry to a victim's devices or systems – through hacking, phishing websites, malware – then deceive the victim into transferring money into their bank account.

SOCIAL ENGINEERING

Criminals can target their victims based on information they share on social media platforms.

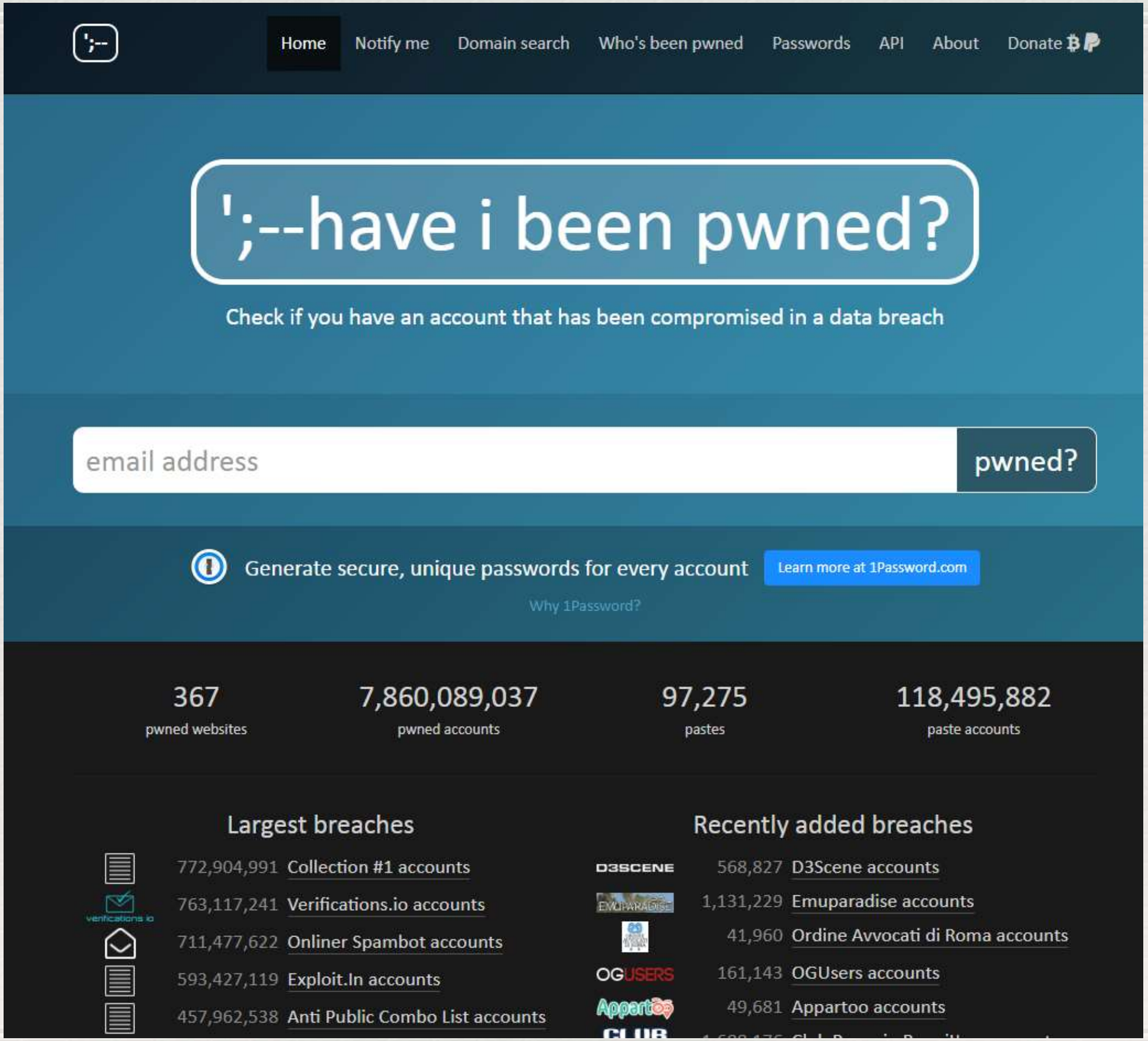
URGENT REQUEST

The criminal impersonates a supplier requesting an urgent payment or change to banking details, or a senior employee in the company with authority to authorize payments.

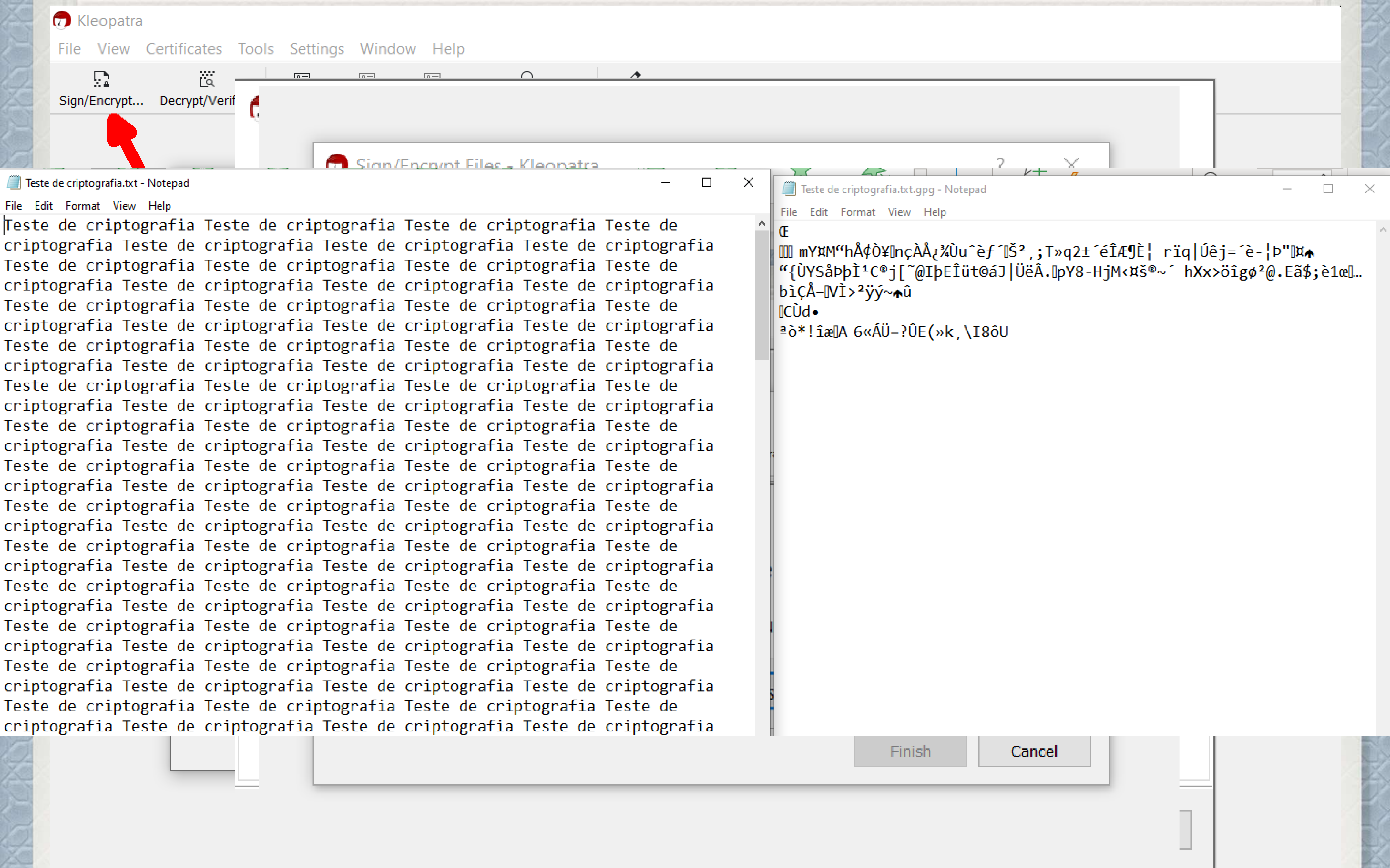
#BECareful

INTERPOL

https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud



https://haveibeenpwned.com/



Add to Archive

Archive: D:\OneDrive\Documentos\Apresentações\2020 - OEA MPF\

Extract : D:\OneDrive\Documentos\Apresentações\2020 - OEA MPF\Teste de criptografia.zip

Extract to:

D:\OneDrive\Documentos\Apresentações\2020 - OEA MPF\

...

Teste de criptografia\

Path mode:

Full pathnames

Eliminate duplication of root folder

Overwrite mode:

Ask before overwrite

Password

Show Password

Restore file security

OK Cancel Help

OK Cancel Help

Senhas mais comuns de 2020

Position	Password	Number of users	Time to crack it	Times exposed
23. ↑ (39)	123321	73,506	Less than a second	928,060
24. ↑ (36)	654321	69,148	Less than a second	953,549
25. ↓ (22)	qwertyuiop	64,632	Less than a second	1,108,463
26. (new)	qwer123456	58,096	4 Seconds	5,339
27. ↑ (158)	123456a	57,472	Less than a second	980,190
28. ↑ (197)	a123456	55,548	Less than a second	684,476
29. ↑ (57)	666666	53,146	Less than a second	889,482
30. ↑ (35)	asdfghjkl	52,961	Less than a second	547,528
31. ↓ (26)	ashley	52,031	2 Minutes	440,413
32. ↑ (58)	987654321	50,097	Less than a second	599,177
33. (new)	unknown	47,995	17 Minutes	28,930

https://nordpass.com/most-common-passwords-list/

Exemplo de *passphrase*

OSemPnmf!A3fqassv202011

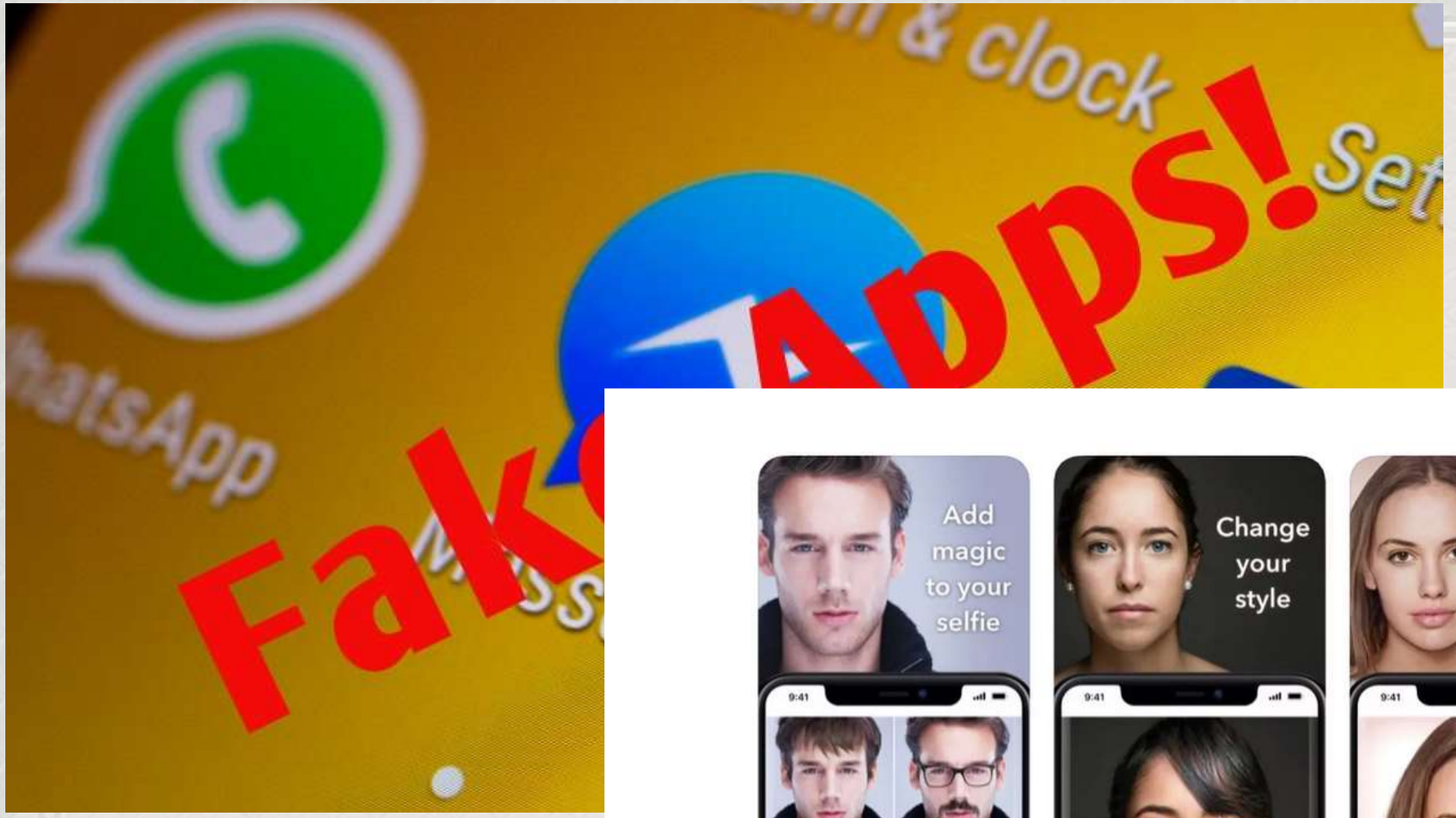
O	Amor
Senhor	é
é	fogo
meu	que
Pastor	arde
nada	sem
me	se
faltará	ver

Dicas (1/2)

- *Utilize software de gerenciamento de senhas (LastPass, Keepass, etc)*
- *Nunca utilize software pirata*
- *Sempre mantenha o S.O. e todos os programas atualizados*
- *Não clique em links antes de checar o endereço que está direcionando*
- *Suspeite de mensagens e emails “bons demais” ou “ruins demais”*
- *Observe atentamente as mensagens que o computador exibe*
- *Atenção com **todos** os seus dispositivos (inclusive seu roteador doméstico)*
- *Tome cuidado com o que e com quem compartilha suas informações (redes sociais)*

Dicas (2/2)

- *Medidas de Proteção em Dispositivos Móveis*
  - *Habilite a autenticação de 2 fatores (ou 2 etapas) em todos os aplicativos*
  - *Habilite uma senha/PIN*
  - *Certifique-se quais programas usam GPS*
  - *Realize backup regularmente e mantenha **tudo** atualizado*
  - *Habilite função de deleção após n tentativas de desbloqueio*
  - *Instale software de rastreamento e limpeza remota*
  - *Monitore sessões ativas rotineiramente*



FaceApp

FaceApp, a Russia-based app that applies filters to photos, is having another moment in the spotlight this week. The app first went viral in 2017, but this time it's catching on because of a filter that makes users look older or younger. As with the last viral moment, however, users

E tem o PIN do
SIM card...

Não se descuide

facebook

Precisa de outra forma de autenticação?

Como encontrar o Gerador de Códigos

1. Abra o aplicativo do Facebook no seu celular
2. Toque em ☰. **Mais**
3. Role a tela para baixo e toque em **Gerador de Códigos**, em **Ajuda e configurações**

Aprovar usando outro dispositivo

Basta verificar suas notificações em outro navegador ou telefone onde você se conectou.

Usar SMS

Enviar para mim o código de login por mensagem de texto

Outras opções

- Enviar uma solicitação para o Facebook

tentasse

baixo.

Continuar

fe.seg.br

#FIQUE ESPERTO

USE UMA SEN
UMA FRASE
VÁRIAS PALA
MEMORIZAÇ
VÁRIOS CAR
ESPECIAIS

SEMPRE HABILITE OS MECANISMOS DE DUPLA AUTENTICAÇÃO FORNECIDOS, POR MEIO DE OUTRAS FERRAMENTAS DE AUTENTICAÇÃO OU MESMO VIA SMS, ESPECIALMENTE NOS APLICATIVOS DE MENSAGENS E REDES SOCIAIS. DESSA FORMA, SE ALGUÉM DESCOBRIR SUA SENHA, NÃO CONSEGUIRÁ ACESSAR A CONTA

PROTEJA AS SENHAS. ADOTE UM APLICATIVO DE GESTÃO DE SENHAS, GUARDE EM UM ARQUIVO CRIPTOGRAFADO OU ANOTE NUM PAPEL E GUARDE EM UM LOCAL SEGURO

NUNCA
SEGURA
MENSAG
CONFIÁ
BANCOS
DADOS

PROTEJ
SENHAS
AUTENT

OR DE

https://fe.seg.br/

401-33 >

Text Message
Today, 11:22

#FiqueEsperto, proteja suas senhas: Use senhas longas, evite sequencias simples e nunca forneca senhas p/ telefone ou mensagens. Saiba mais: htt[redacted].br

Foi vítima?

- *Entre em contato com a área de suporte ao usuário*
  - *Para demandas não tratadas localmente => Divisão de Segurança da Informação (SUBINF/STIC/PGR)*
- *Sala de Atendimento ao Cidadão do MPF*
  - *http://www.mpf.mp.br/servicos/sac*
- *Polícia Federal / Polícia Civil*
- *Contato direto (Provedor, Banco, responsável, etc)*
- *Ata Notarial*
- *Contate um advogado especialista e/ou perito digital*

Aspectos práticos

17:47

Ajus

Marcelo
Fructus Laboris

Mensagens favorita

WhatsApp Web/Co

Conta

Conversas

Notificações

Armazenamento e

Ajuda

Convidar um amigo

Status Ligações Câm

17:48

Voltar Confirmação em duas etapas Avançar

Adicione um endereço de e-mail à sua conta para redefinir seu PIN caso você o esqueça e para proteger sua conta. Pular.

E-mail

Marcelo Caiado
mbcaiado@gmail.com

Marcelo Caiado
marcelobc@mpf.mp.br

q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123 espaço @ . seguinte

17:48

Conta Privacidade

Visto por último Ninguém

Foto de perfil Meus contatos

Recado Meus contatos

Grupos Meus contatos

Status 0 selecionados

Localização em tempo real Nenhuma

Conversas onde você compartilhou sua localização em tempo real.

Bloqueados 25 contatos

Lista de contatos que você bloqueou.

Confirmações de leitura

Se desativar as confirmações de leitura, você não poderá ver as confirmações de leitura de outras pessoas. As confirmações de leitura são sempre enviadas para conversas em grupo.

Bloqueio de tela

Exigir o Face ID para desbloquear o WhatsApp.

Status Ligações Câmera Conversas Ajustes

etapas

firmação em duas
do você registrar o
tsApp novamente.

Conversas Ajustes

17:50
◂ Busca

Voltar

Criar Senha

Criar Senha

17:51
◂ Busca

Voltar

Dica

Você pode criar uma dica opcional para a sua senha.

Dica (opcional)

Pular escolha da dica

17:51
◂ Busca

Voltar

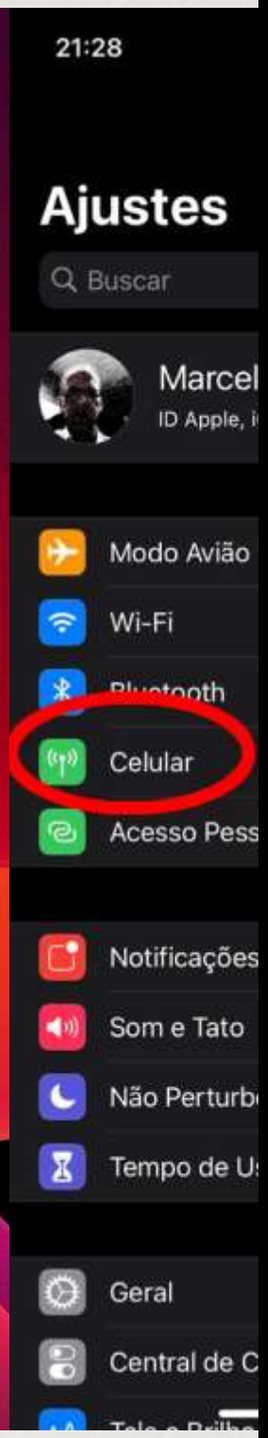
Email de Recuperação

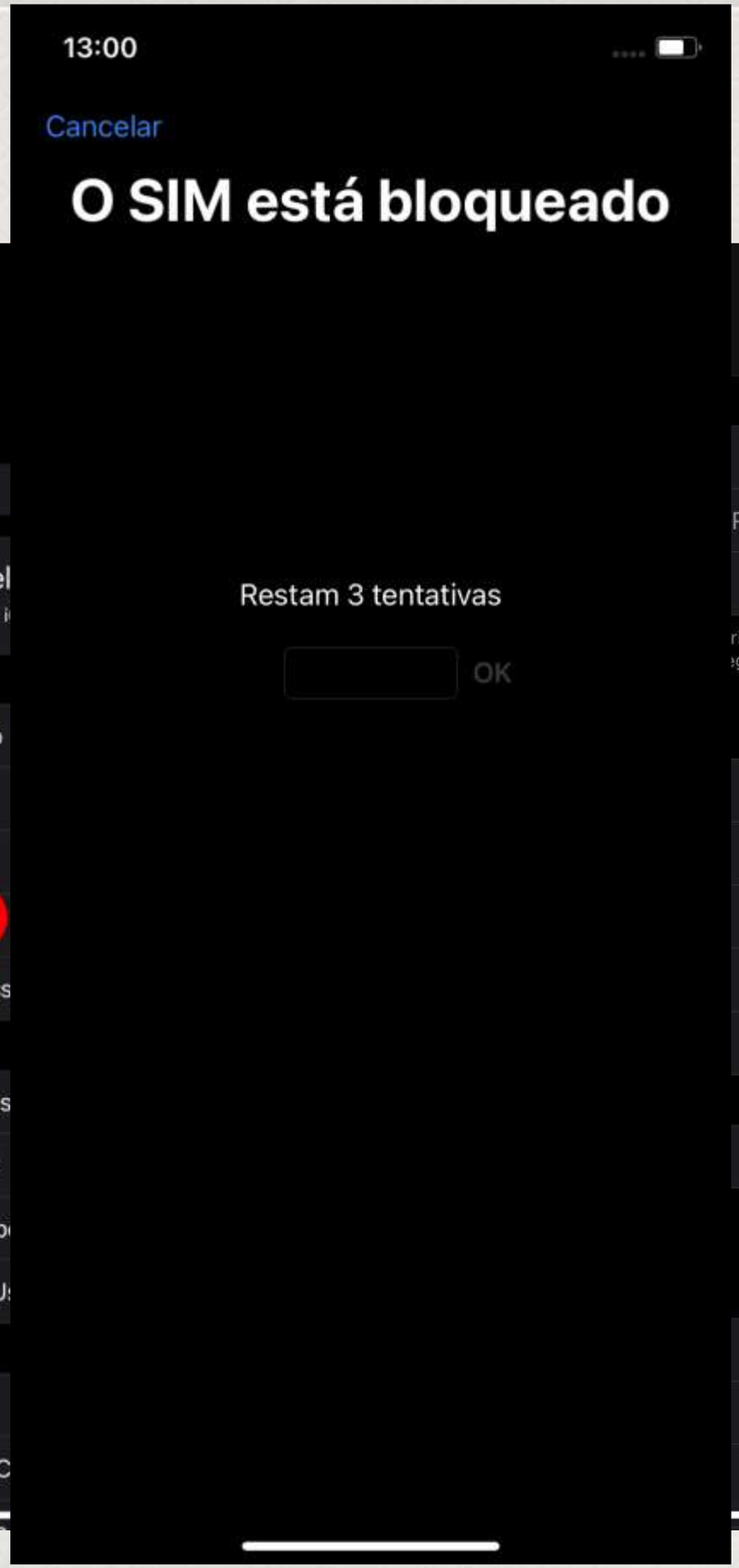
Você pode definir um email de recuperação para ser capaz de redefinir a sua senha e restaurar acesso à sua conta do Telegram.

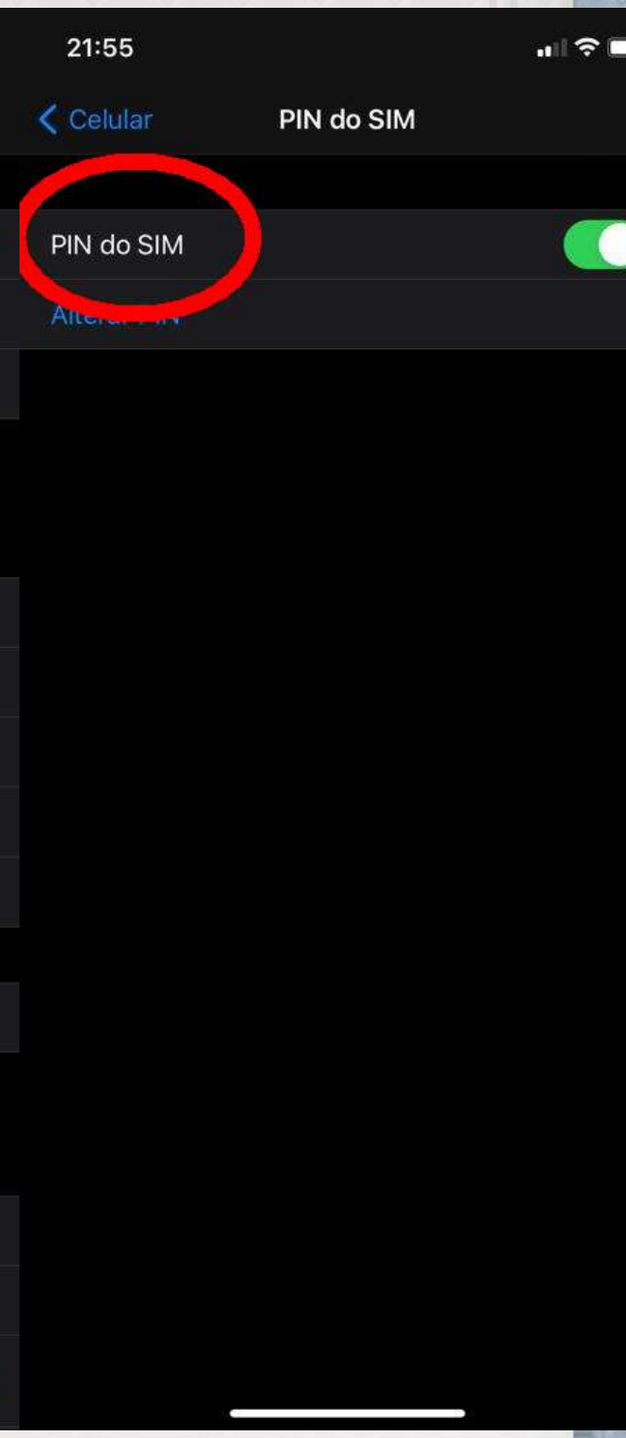
mbcaiado@gmail.com

Continuar

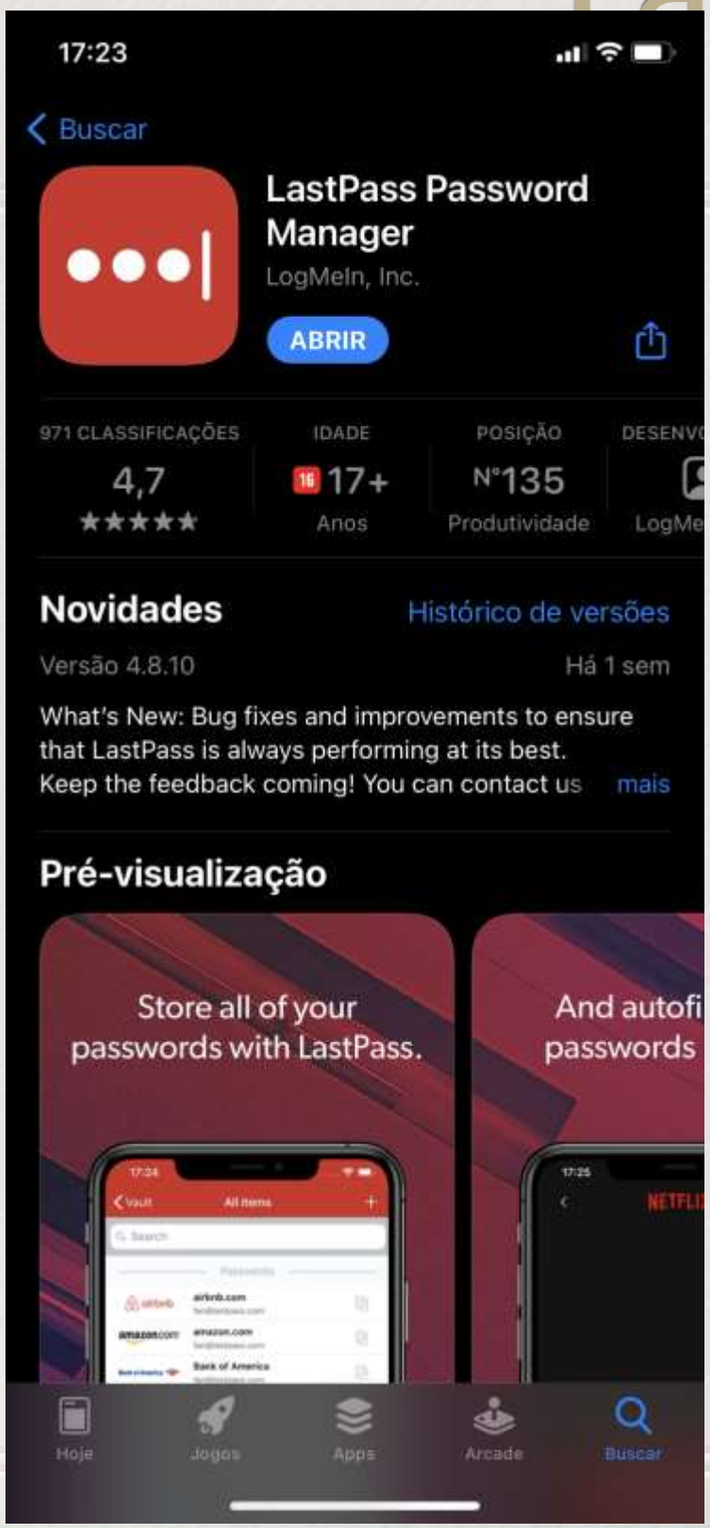
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123 espaço @ . concluído

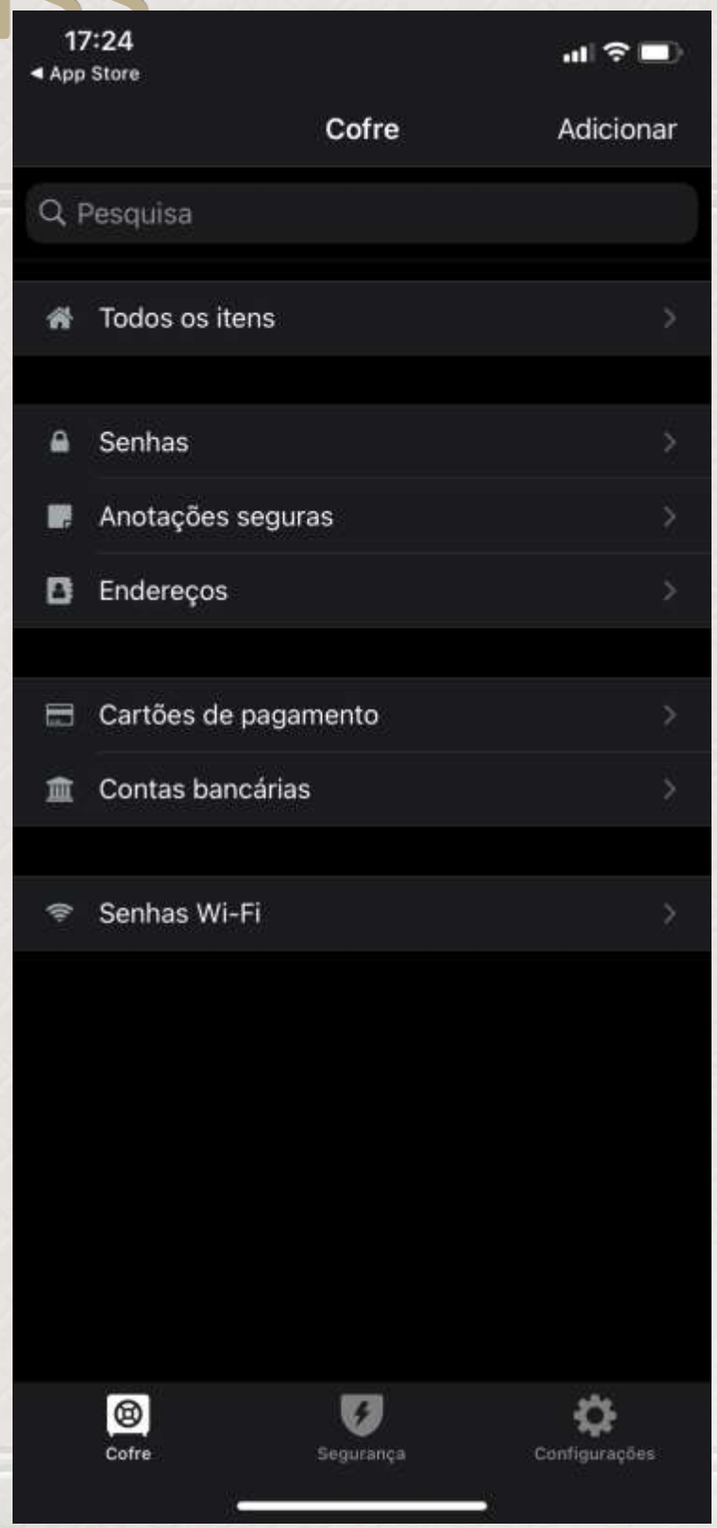






Lastpass





Google Authenticator

Google Conta

Verificação em duas etapas

; outras opções não

A verificação em duas etapas está ATIVADA desde 28 de ago. de 2012

DESATIVAR

gratuitamente,
id e iPhone.

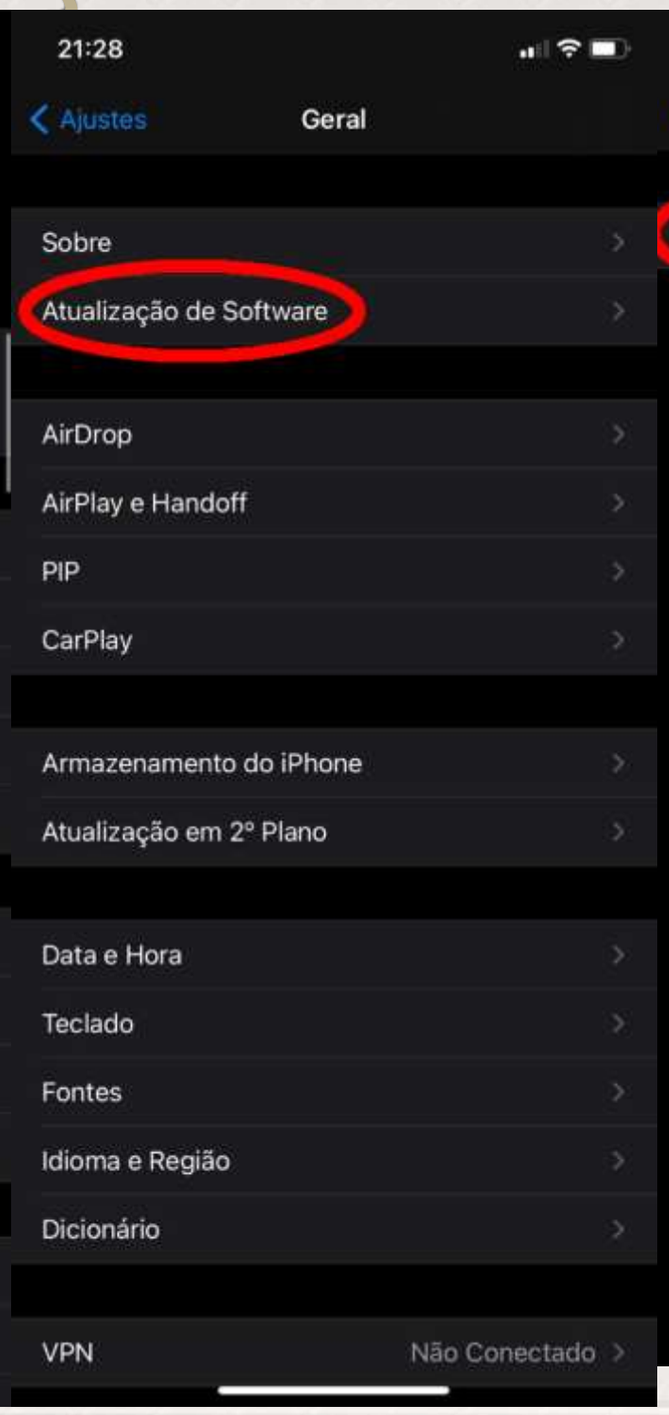
Opções de segunda etapa disponíveis

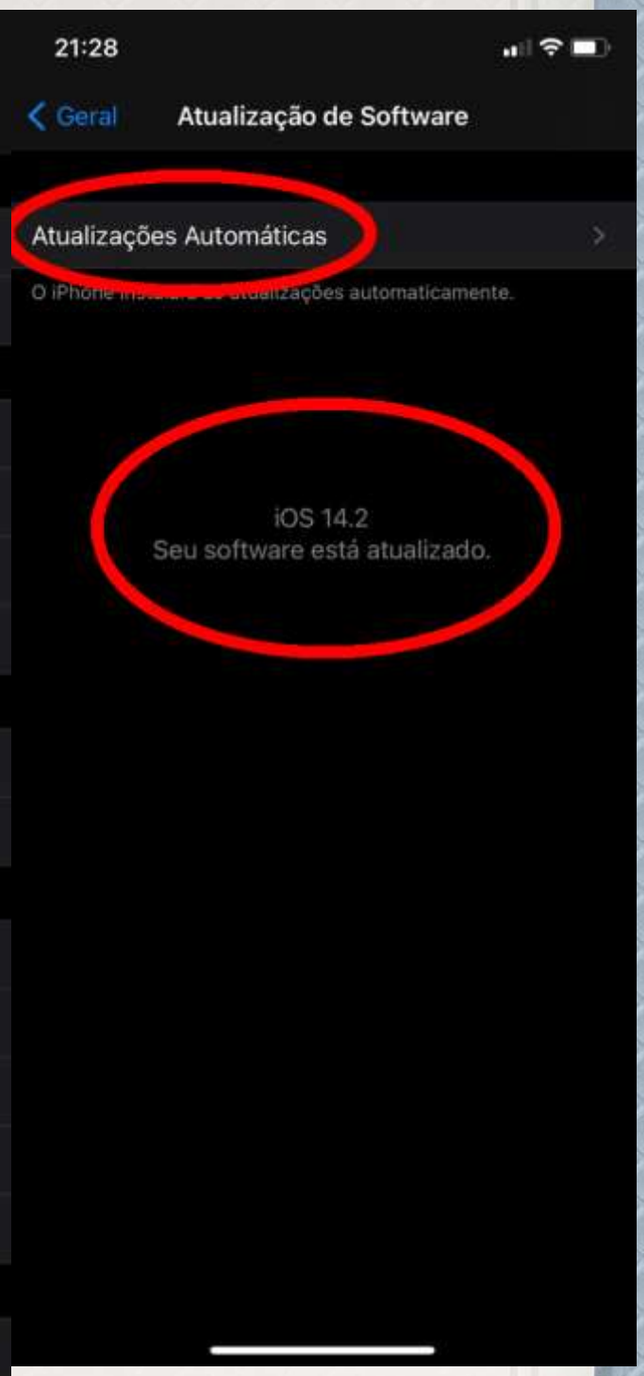
Depois que você digita a senha, uma segunda etapa confirma que é você que está fazendo login.
Saiba mais

ce a você um login ainda
oth ou ser conectada

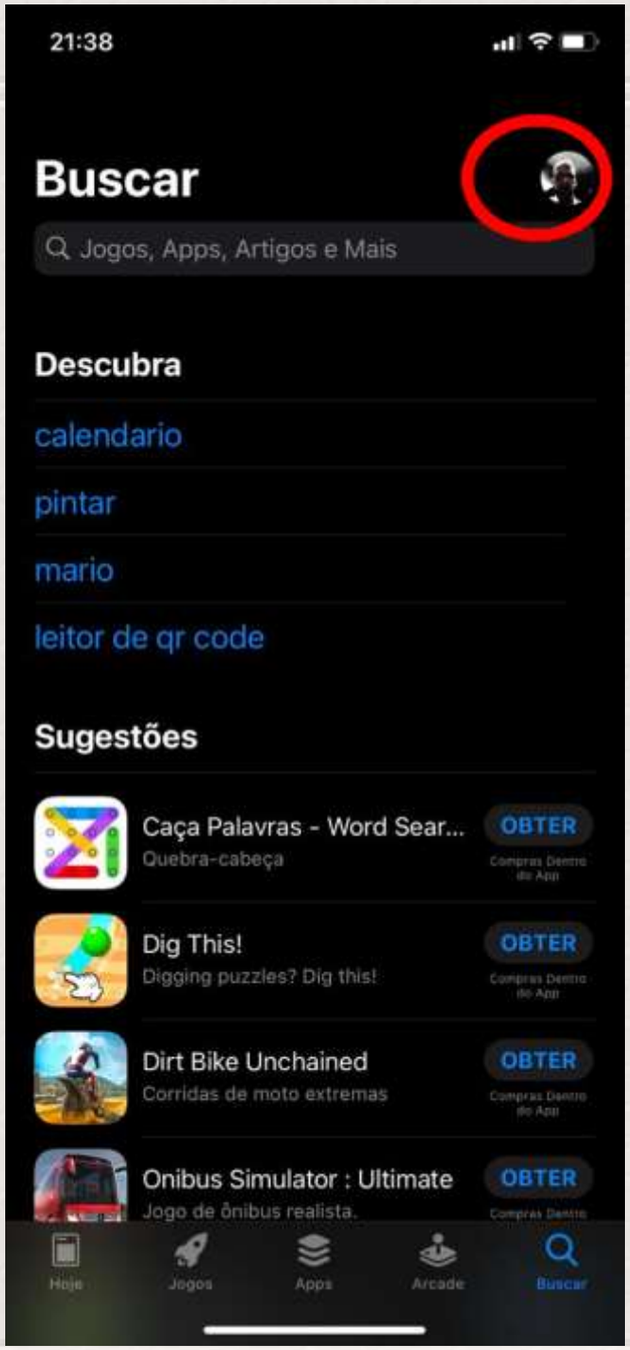
CANCELAR CONFIRMAR

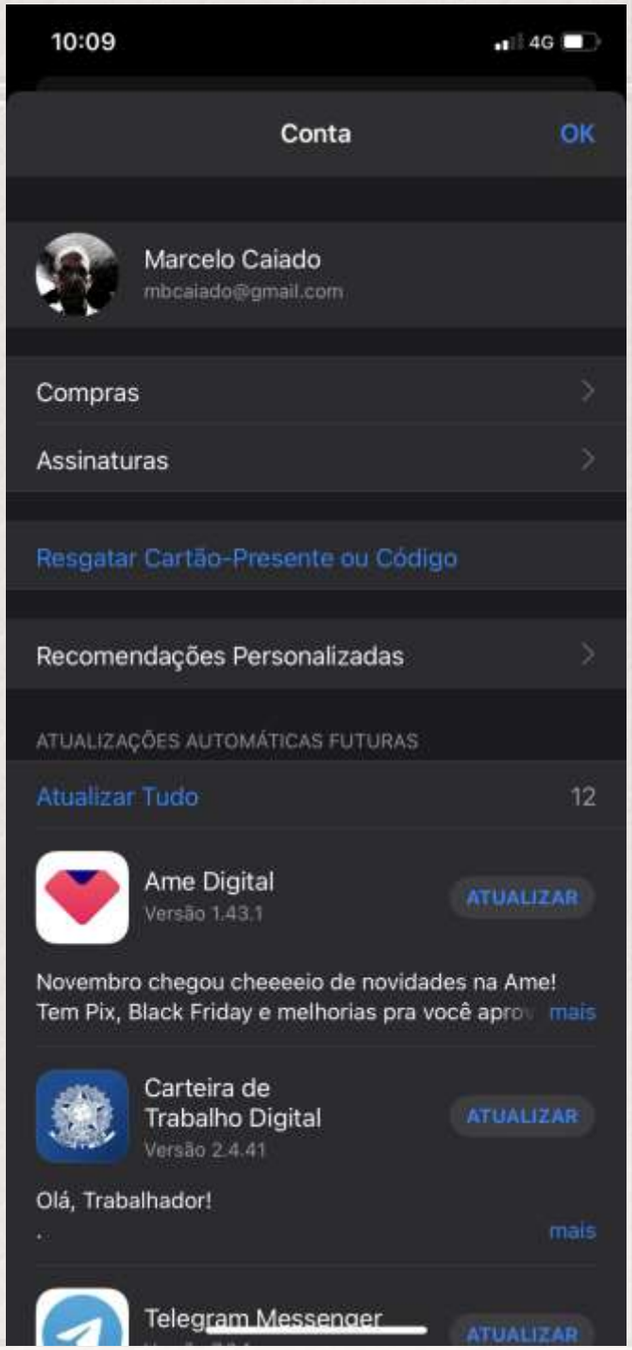
Atualização iOS



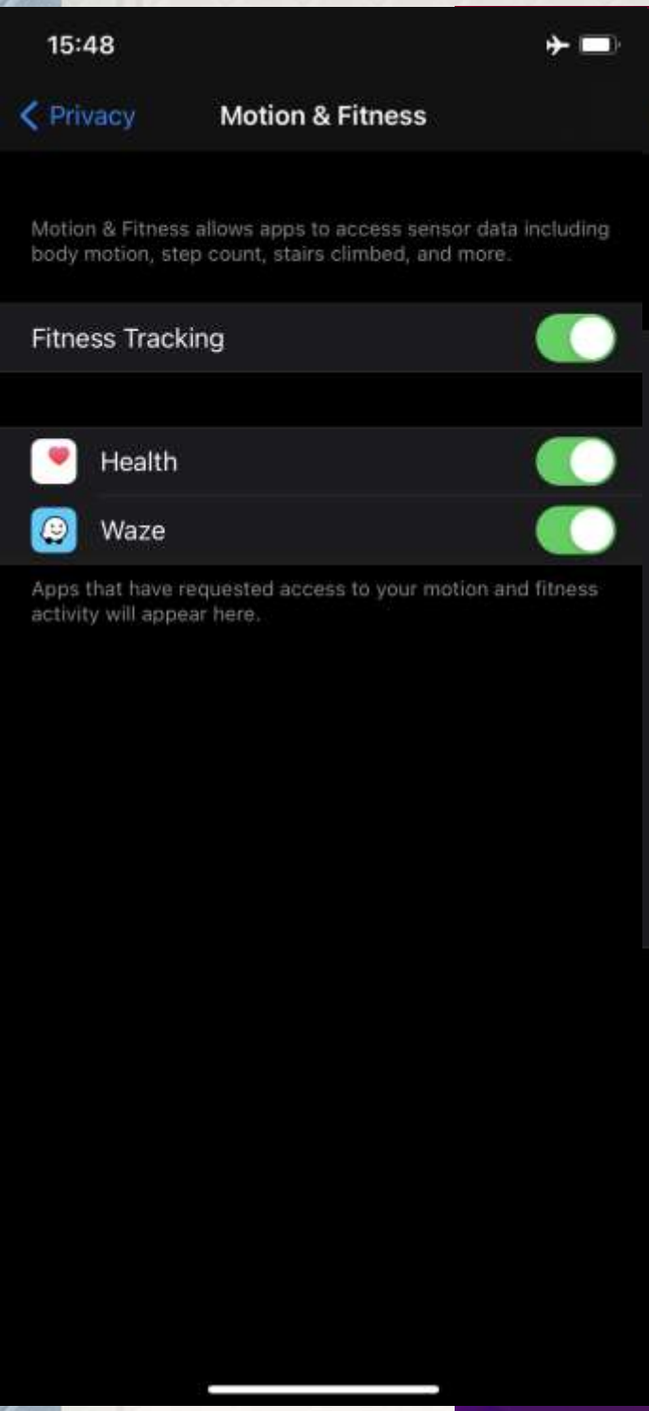


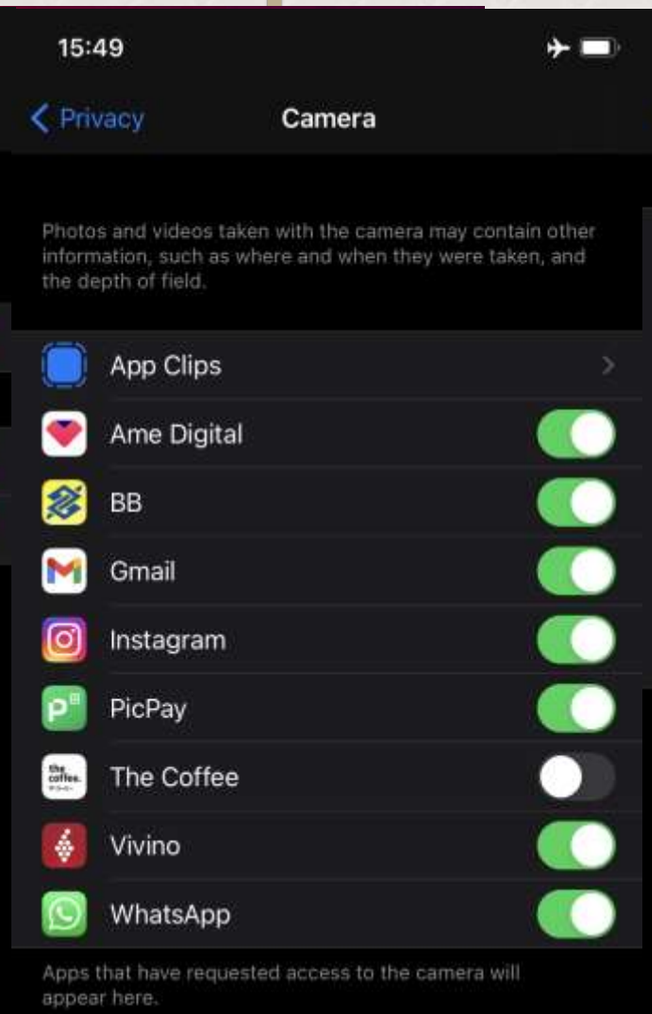
Atualização Apps

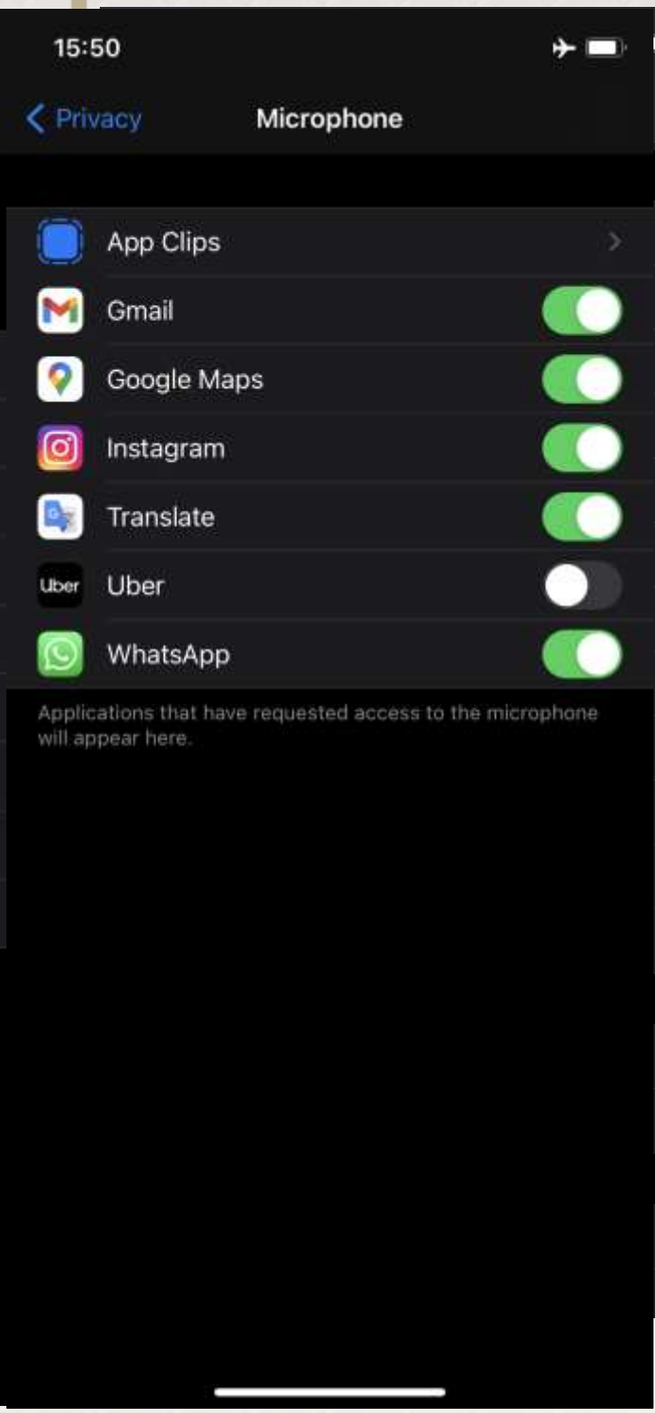


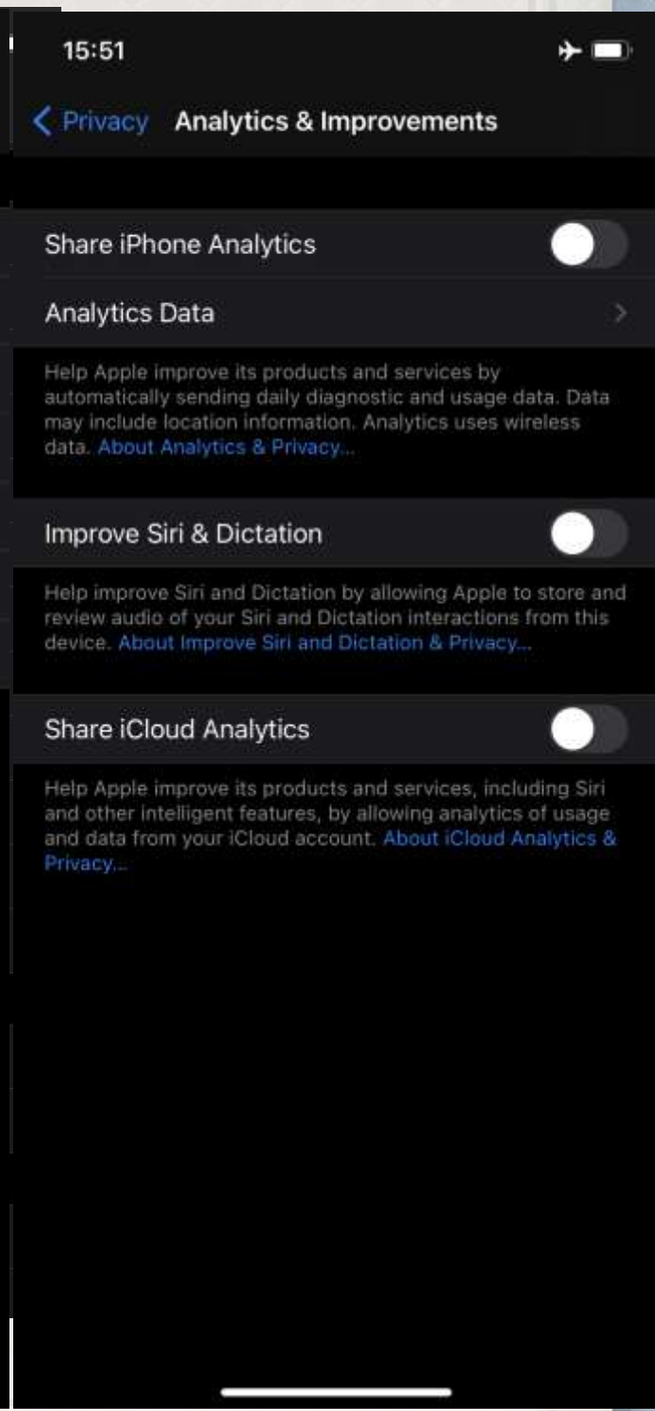


Verifique as permissões









Para refletir

"Mesmo a melhor infraestrutura de segurança da informação não pode garantir que intrusões ou outras ações maliciosas não ocorrerão."

Tradução: CERT/CC CSIRT FAQ
http://www.cert.br/certcc/csirts/csirt_faq-br.html

Perguntas

marcelobc@mpf.mp.br