Crimes e Golpes Digitais
Como Evitá-los?

Marcelo Caiado
Perito em Tecnologia da Informação e Comunicação
M.Sc., CISSP, GCFA, GCIH, GSLC, CHFI, CEI
http://dfir.com.br

Disclosure

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

Apresentação

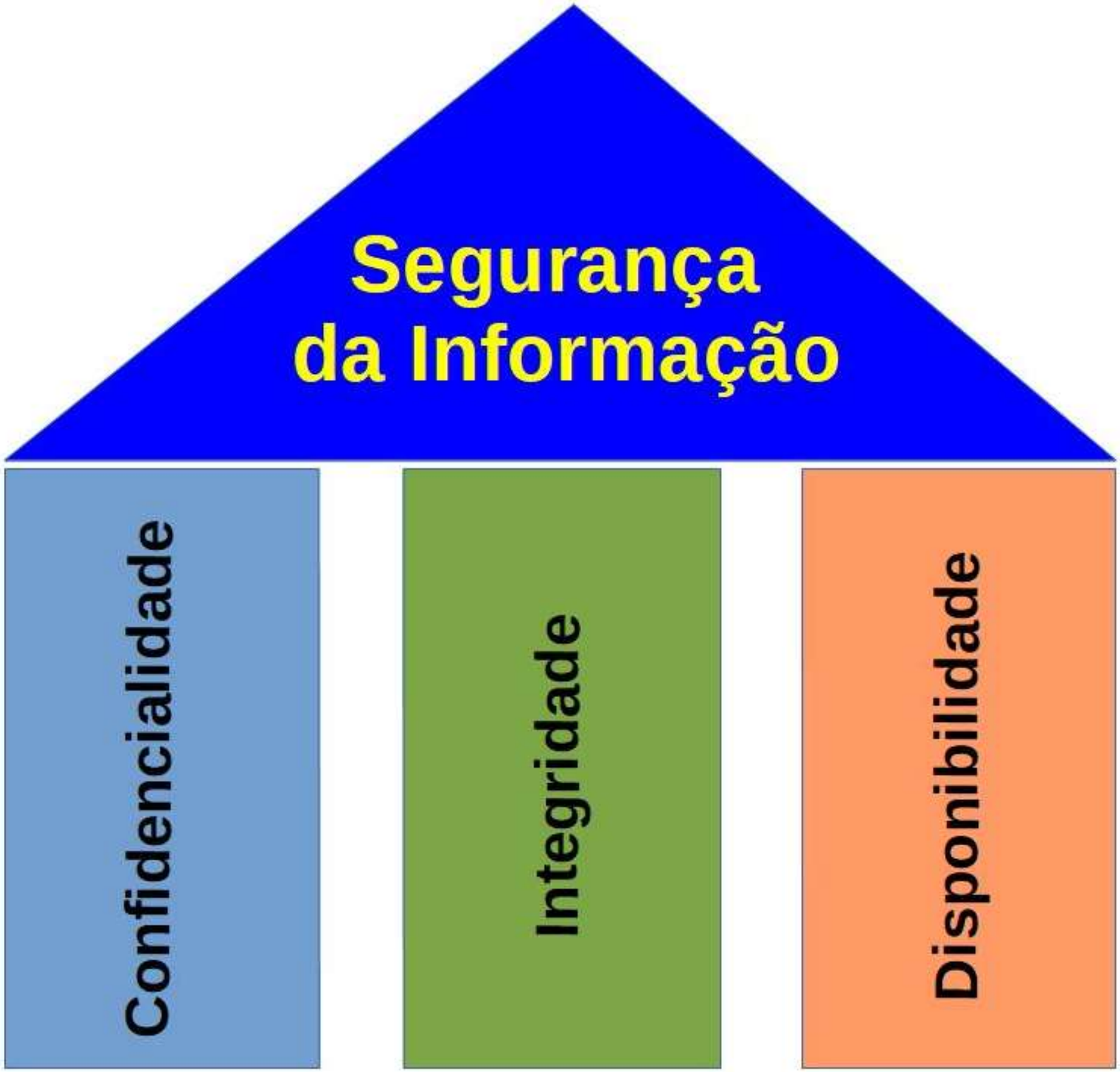
- *Graduado em Processamento de Dados (UCB) e em Administração de Sistemas de Informações (UNEB)*
- *Especialista em Gestão Pública (FGV)*
- *Mestre em Ciência da Computação (UnB)*
- *Analista do MPU / Perícia / TIC (1997)*
- *CyberForensics Analyst / Blackberry – 2008 a 2010*
- *Mantenedor do site*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

Foto de Bruno Scramgnon no Pexels

Estatísticas do IC3

Fonte: IC3 2019 Internet Crime Report (FBI)

“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.”


Segurança
da Informação
Confidencialidade
Integridade
Disponibilidade

Golpistas invadem WhatsApp de cantora e mandam mensagens para contatos dela pedindo dinheiro

Criminoso se passou por assessor e pediu dados pessoais para invadir celular da vítima. Jornal de Brasília já havia not
cantor local

JBr
Publicado 2 meses atrás em 21/01/2020
Por Redação Jornal de Brasília

E

Crime de invasão (1)

Art. 307 do Código Penal (Decreto Lei 2.848/40)

- Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
  - Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Crime de invasão (2)

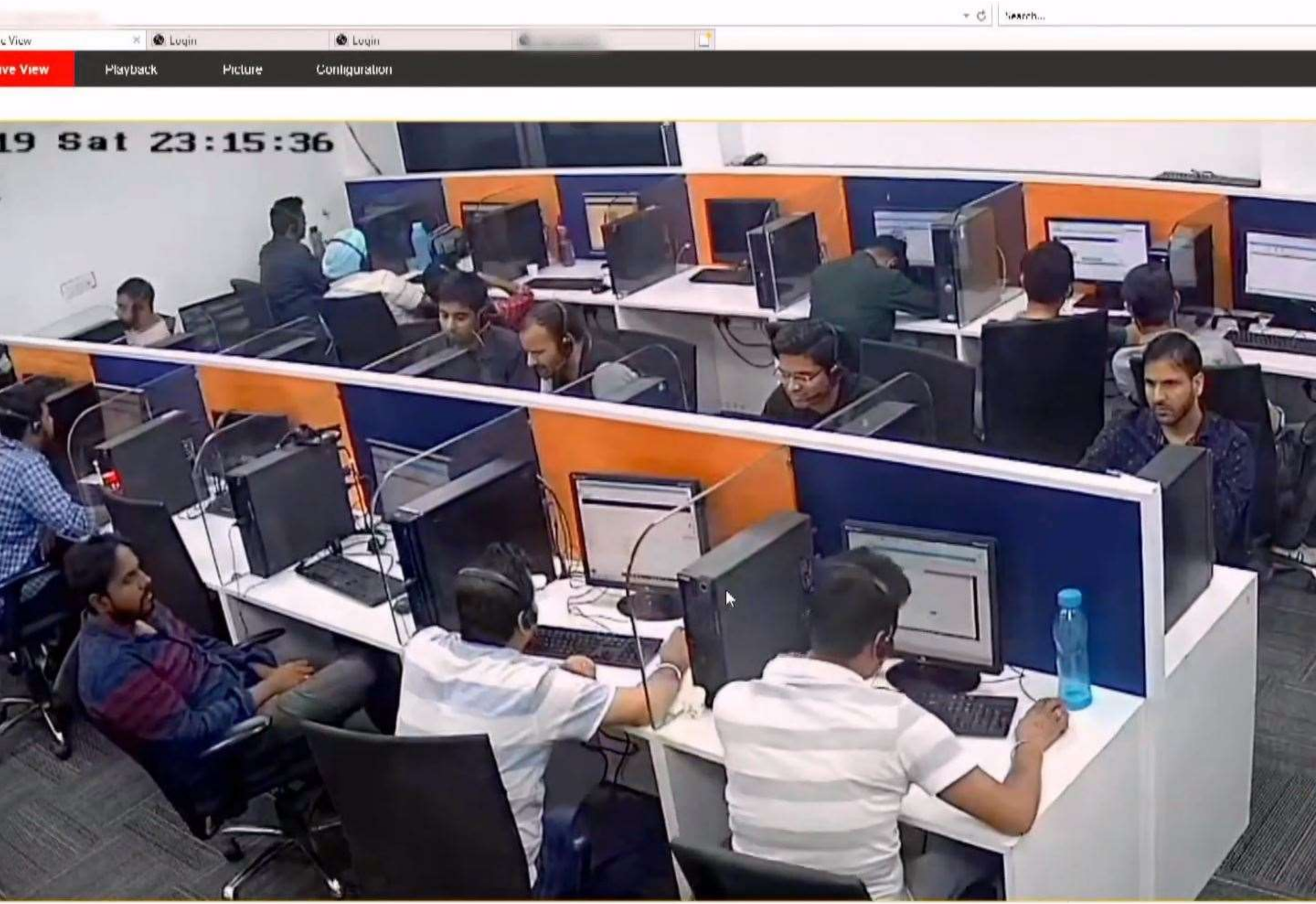
Art. 154-A da Lei 12.737/12

- Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
  - Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Crime de invasão (3)

Art. 10 da Lei 9.296/96

- Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
  - Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.



©2018 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

You're calling Online Technical Support.
This is Mary. How may I help you today?

INDÚSTRIA

PCs com Windows 7 estarão mais vulneráveis a ransomware a partir de 14 de janeiro

LUIZ QUEIROZ 9 DE JANEIRO DE 2020

NEGLIGÊNCIA

*A informação é da Veritas [illegible] Imprensa –

Os computadores que ainda estiverem executando o Windows 7 quando este chegar ao fim da sua vida útil, em [illegible] de janeiro, estarão significativamente maior de sofrer ataques de ransomware, alerta a Veritas [illegible] Segundo especialistas, espera-se que 26% dos PCs ainda estejam executando o software da Microsoft após o término do suporte.

A vulnerabilidade à ransomware de PCs que executam softwares sem suporte foi demonstrada pelo vírus WannaCry em 2017. Apesar dos computadores suportados receberem correções contra cryptoworm, a Europol estima que 200 mil dispositivos em 150 países, executando um software mais antigo e sem suporte, foram infectados pelo WannaCry.

E, embora apenas US $ 130 mil tenham sido pagos em resgate, entende-se que o impacto nos negócios chegou a bilhões de dólares devido à perda de produtividade e de dados, além de hardwares corrompidos.

Capi
Digi

MICROSOFT
CO

STF ADIA PAR
DE ESTAT

Funcionária do governo dos EUA renuncia após vazamento de dados federais

© AP Photo / Susan Walsh

MUNDO 14:37 10.07.2015 (atualizado 10:14 05.10.2015) URL curta

0 3 1

Nos siga no Google News

A diretora do Escritório de Administração de Pessoal (OPM, na sigla em inglês), agência ligada ao governo dos Estados Unidos, anunciou nesta sexta-feira a sua renúncia, depois de um devastador vazamento de dados pessoais de milhões de funcionários federais, no mês passado.

"Eu transmiti ao presidente (Barack Obama) que acredito ser melhor para mim ficar de lado e permitir que a nova liderança chegue, fazendo com que a agência supere os desafios atuais", declarou Katherine Archuleta

09/03 17:30 Como queda do petróleo está afetando economia brasileira e internacional?

09/03 16:43 Escritor Paulo Coelho homenageado em Portugal com escultura de artista russo

09/03 16:39 Bolsonaro diz que governo não irá interferir em política de preços da Petrobras

09/03 15:50 Colisão de ônibus deixa quase 30 mortos em Gana

09/03 14:37 Crise de coronavírus pode custar

Dona do Financial Times perde US$ 29M em golpe via email

Da Redação 06/11/2019

No golpe contra a Nikkei America os bandidos se fizera
conseguiram a transferência de US$ 29 milhões para u

fraudadores que exploram a confiança dos funcionári
não forneceu detalhes específicos, dizendo apenas qu
havia notificado as autoridades nos EUA e em Hong K
nesse tipo de golpe).

"Estamos investigando e verificando os detalhes dos f
comunicado. A empresa publica o índice de ações Nik

Fundada em 1876, a Nikkei Inc. é uma marca de mídia
Emprega cerca de 1.500 jornalistas em todo o mundo
Financial Times em 2015 por US $ 1,3 bilhão.

Comprometimento de e-mails corporativos pode custar milhões

Toyota perde US$ 37 milhões em um ataque BEC. Saiba mais sobre os perigos do comprometimento dos e-mails corporativos e como evitar que sua empresa seja vítima.

Nikolay Pankov 11 out 2019

https://phishingquiz.withgoogle.com/?hl=pt-BR

TEL AVIV – The IDF foiled a honeypot network with false social media profiles of attractive young women created by the Hamas terror group and designed to dupe IDF soldiers, the third such operation in as many years.

Hundreds of soldiers had their phones compromised in the latest honeypot attempt.

(photo credit: IDF SPOKESPERSON'S UNIT)

The operation consisted of six "women" posing provocatively: Sara Orlova, Maria Jacobova, Eden Ben Ezra, Noa Danon, Yael Azoulay and Rebecca Abuksis. Most of them went to some lengths to explain their poor Hebrew, either presenting themselves as new immigrants to Israel or else saying they have hearing or vision impairments.

469 comments

Joe Biden Gets Endorsement from Bloomberg Gun Control Group

246 comments

Italy Quarantines 16 Million People in Attempt to Contain Coronavirus

3471 comments

Donald Trump Shakes Hands with Supporters Despite Coronavirus Fears

463 comments

Bette Midler Blasts Trump: Doesn't Want 'Coronavirus' Cases to 'Go Up'

965 comments

Carney: 9 Things Trump Can Do To Save the Economy from Coronavirus

1327 comments

D.C. Reverend Gave Communion Before Coronavirus Diagnosis

878 comments

ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $2,500,000						
Up to $2,000,000						
Up to $1,500,000						
Up to $1,000,000						
Up to $500,000	3.001 Persistence (iOS)	2.005 WeChat RCE+LPE (iOS/Android)	2.006 iMessage RCE+LPE (iOS)	2.007 FB Messenger RCE+LPE (iOS/Android)	2.008 S RC	
Up to $200,000	5.001 Baseband RCE+LPE (iOS/Android)		6.001 LPE to Kernel/Root (iOS/Android)	2.011 Media Files RCE+LPE (iOS/Android)	2.012 Do RC	
Up to $100,000	7.001 Code Signing Bypass (iOS/Android)	5.002 WiFi RCE (iOS/Android)	5.003 RCE via MitM (iOS/Android)	6.002 LPE to System (Android)	8.001 Info Dis	

1.001 Android FCP Zero Click (Android)
1.002 iOS FCP Zero Click (iOS)
2.001 WhatsApp RCE+LPE Zero Click
2.002 iMessage RCE+LPE Zero Click

* All payouts are subject to change or cancellation without notice. All trademarks are the pro

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000											1.001 Win RCE Zero Click (Win)
Up to $500,000								3.001 Chrome RCE+LPE (Win)	2.001 Apache RCE (Linux)	2.002 MS IIS RCE (Win)	
Up to $250,000							5.001 MS Outlook RCE (Win)	4.001 MS Exchange RCE (Win)	2.003 OpenSSL RCE (Linux)	2.004 PHP RCE (Linux)	
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE (Win/Linux)				4.002 Sendmail RCE (Linux)	4.003 Postfix RCE (Linux)	4.004 Dovecot RCE (Linux)	4.005 Exim RCE (Linux)	2.005 nginx RCE (Linux)	
Up to $100,000		3.002 Safari RCE+LPE (Mac)	3.003 Edge RCE+LPE (Win)	3.004 Firefox RCE+LPE (Win)		5.003 Word/Excel RCE (Win)	7.001 WordPress RCE (Linux)	7.002 cPanel/WHM RCE (Linux)	7.003 Plesk RCE (Linux)	7.004 Webmin RCE (Linux)	
Up to $80,000	6.002 VMware WS VME (Win/Linux)						5.004 Adobe PDF RCE+SBX (Win)	5.005 WinRAR RCE (Win)	5.006 7-Zip RCE (Win)	6.003 Windows LPE/SBX (Win)	
Up to $50,000	6.004 USB LPE (Win/Mac)	8.001 Antivirus RCE (Win)				5.007 WinZip RCE (Win)	5.008 tar RCE (Linux)	6.005 macOS LPE/SBX (Mac)	6.006 Linux LPE (Linux)	6.007 BSD LPE (BSD)	
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE (Win)	7.005 phpBB RCE (Linux)	7.006 vBulletin RCE (Linux)		7.007 MyBB RCE (Linux)	7.008 Joomla RCE (Linux)	7.009 Drupal RCE (Linux)	7.010 Roundcube RCE (Linux)	7.011 Horde RCE (Linux)	

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

ibeenpwned.com

Home Notify me Domain search Who's been pwned Passwords API About Dona

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

br2can@gmail.com

pwne

Oh no — pwned!

Pwned on 8 breached sites and found no pastes (subscribe to search sensitive breaches)

Google Authenticator

Google LLC Tools

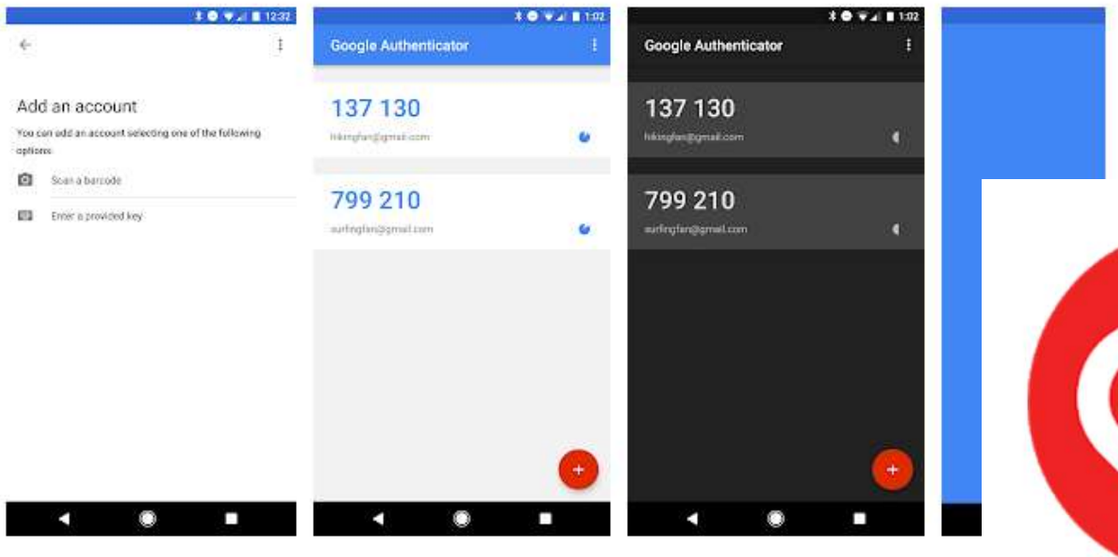
★★★★☆ 192,872

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

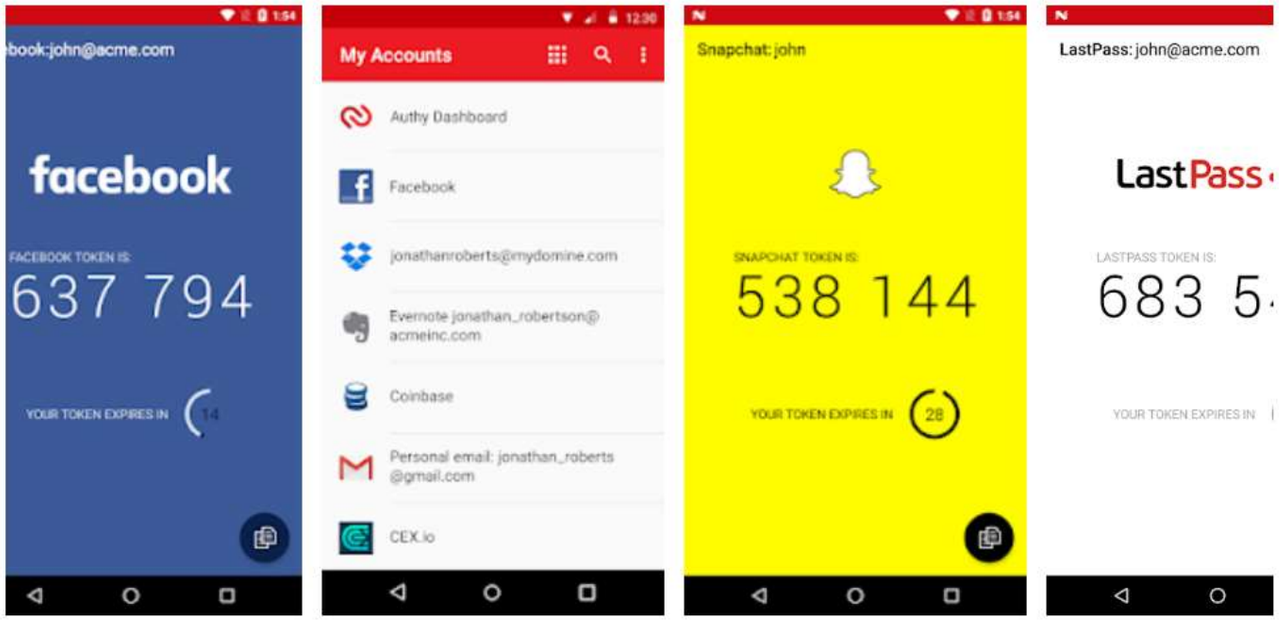
Everyone

This app is compatible with your device.

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

Add to Wishlist

Install



ESPELHAMENTO INDEVIDO DE APLICATIVO

Verifique as Sessões Ativas

DPC ALESANDRO BARRETO @DELBARRETO19

WHATSAPP

IOS

- Abra o aplicativo;
- Ajustes;
- WhatsApp Web/Desktop;
- Dispositivos com sessões ativas.

ANDROID

- Abra o aplicativo;
- Clicar em ... no canto superior;
- WhatsApp Web;
- Sessões ativas.

TELEGRAM

IOS

- Abra o aplicativo;
- Configurações;
- Privacidade e Segurança;
- Sessões ativas.

ANDROID

- Abra o aplicativo;
- Configurações;
- Privacidade e Segurança;
- Sessões ativas.

DICAS

- Habilite a verificação de 2ª etapa no aplicativo;
- Verifique, com frequência, as sessões ativas no seu smartphone.

TODOS OS DIREITOS RESERVADOS

CLONAGEM DE WHATSAPP

DELEGADO ALESANDRO BARRETO

PROTEJA SUA CONTA
HABILITE VERIFICAÇÃO 2ª ETAPA

@DELBARRETO19

CONTEXTUALIZAÇÃO

Os golpes praticados com a clonagem de simcard aumentaram consideravelmente nos últimos meses. A habilitação por parte do usuário de verificação de 2ª etapa da conta do WhatsApp dificulta, sobremaneira, a atuação do criminoso.

IPHONE

- Acesse o WhatsApp;
- Ajuste;
- Conta;
- Verificação em duas etapas;
- Ativar;
- Inserir pin com 06 dígitos;
- Infome email para recuperação.

ANDROID

- ...
- Configurações;
- Conta;
- Verificação em duas etapas;
- Ativar;
- Inserir pin com 06 dígitos;
- Informe email para recuperação.

TODOS OS DIREITOS RESERVADOS

Fonte: Cybercards – Meio Cibernético: Orientações Práticas / Delegado Alessandro Barreto

virustotal.com/gui/file/c4f22c523a299d4b96643de5c6e8a5b93bc4b87152d2fd0f0ee6424ebb4ecf50/detection

a5b93bc4b87152d2fd0f0ee6424ebb4ecf50

4 / 70

Community Score

4 engines detected this file

c4f22c523a299d4b96643de5c6e8a5b93bc4b87152d2fd0f0ee6424ebb4ecf50

Setup

overlay | peexe | runtime-modules | signed

54.06 MB
Size

2020-03-11 16:20:35 UTC
a moment ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY

Antiy-AVL	Trojan/Win32.Wacatac	Jiangmin	Trojan.PSW.Predator.arf
Yandex	Trojan.PWS.Predator!	Zillya	Trojan.GenKryptik.Win32.40518
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
SecureAge APEX	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	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
Cyren	Undetected	DrWeb	Undetected

spyware
detection
internet
infected
virus
international
trojan
phishing
hacker
infection
firewall
cyber
spam
intruder
malware
hackers
networks
service
target
hacking
attack
crime
network
access
people
rooms
using
needed
altering
criminal
between
services
directly
defined
counts
included
technical
unauthorized
individuals
mail
content
crimes
communications
child
pornography
system
information
activities
computer
groups
theft
terrorist
victim
infected
organized

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

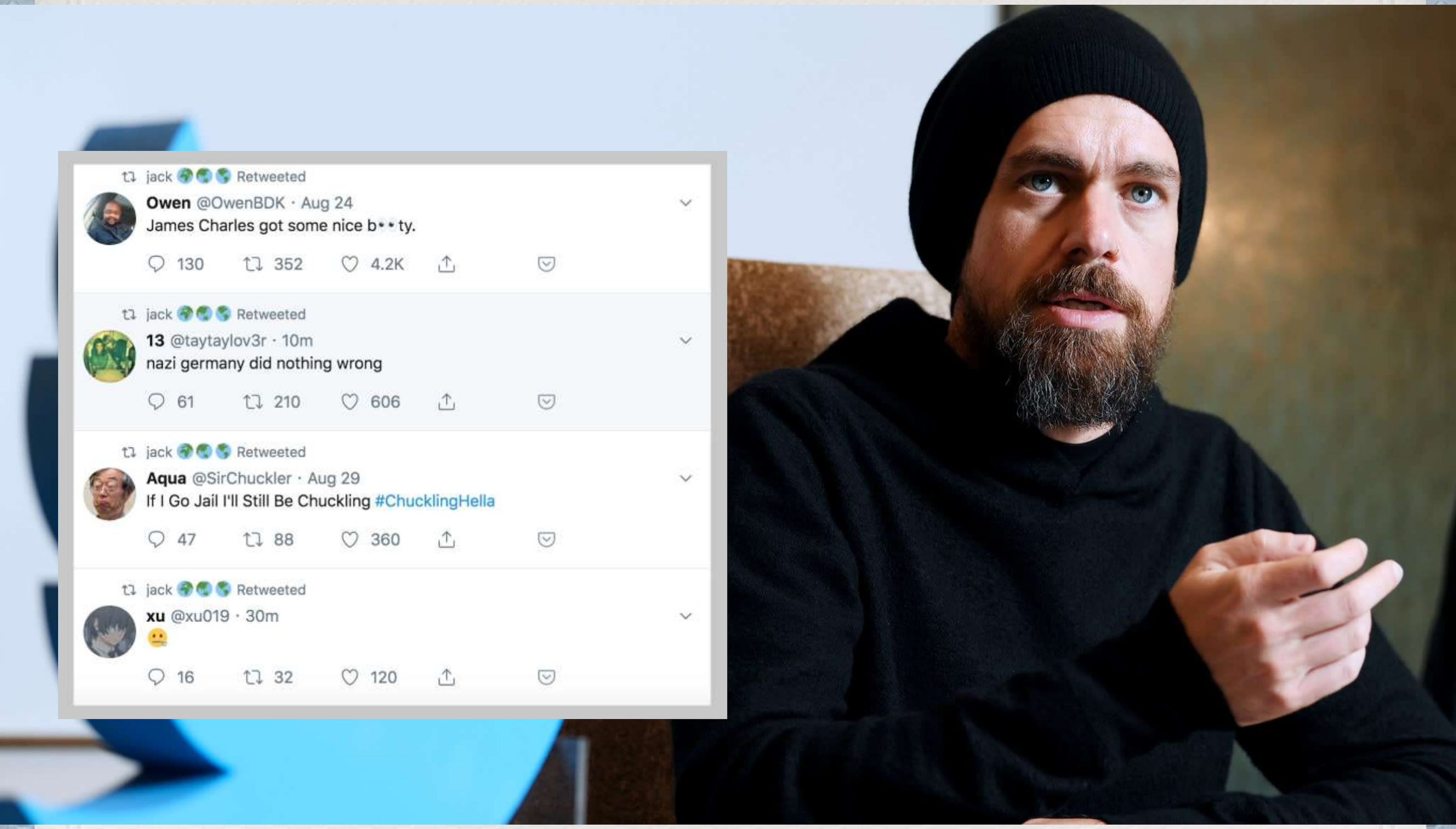
*Atenção com **todos** os seus dispositivos (inclusive seu roteador doméstico)*

Tome cuidado com o que e com quem compartilha suas informações (redes sociais)

Dicas (2/2)

Medidas de proteção em dispositivos móveis

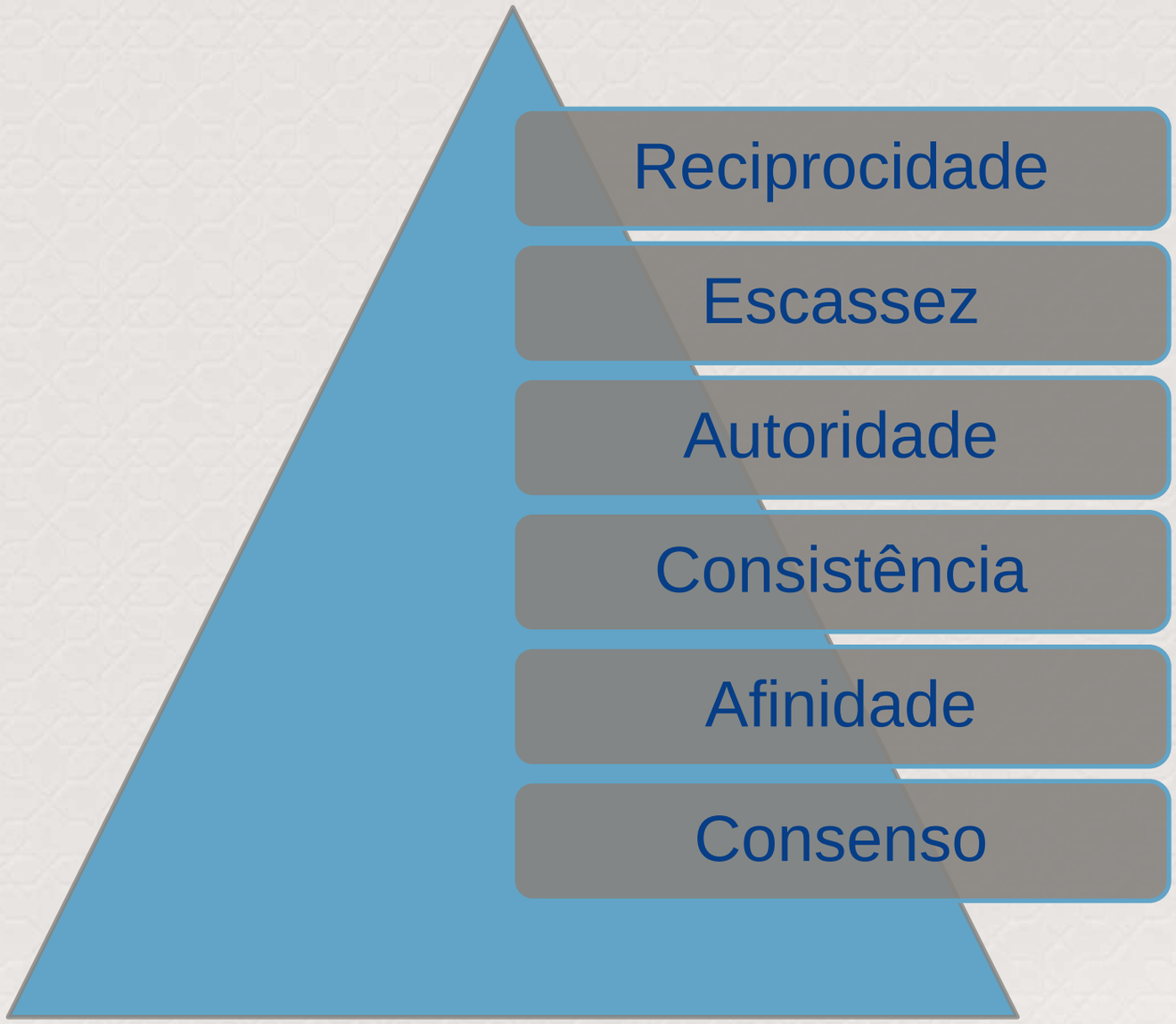
- *Habilite a autenticação de dois fatores (app) em todos os aplicativos*
- *Habilite uma senha segura*
- *Certifique-se quais programas usam GPS*
- *Realize backup regularmente e mantenha **tudo** atualizado*
- *Habilite função de deleção após n tentativas de desbloqueio*
- *Instale software de rastreamento e limpeza remota*
- *Habilite a criptografia no dispositivo e no cartão de memória*
- *Desative o seu correio de voz*



Conta do Jack Dorsey, CEO do Twitter, hackeada por ***SIM Swap (30/08/19)***

E tem o PIN do SIM card...

Engenharia Social



Boatos: Na dúvida, não compartilhe!

Dentre tantas notícias que circulam por aí, fica difícil saber no que acreditar.

O **Fascículo Boatos** apresenta dicas para tentar ajudá-lo a identificar um boato, afinal, quem repassa boatos pode ser responsabilizado pelos danos causados, pode passar vergonha e perder a credibilidade.

Lembre-se: Independente do nome recebido, os boatos geram desinformação, causam problemas e precisam ser combatidos.

Você sabe o que é *ransomware*? Você tem *backup*?

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

Saiba mais:
https://cartilha.cert.br/ransomware/

Guias Internet Segura

Confira o **Guia Internet Segura**, com dicas para que as crianças possam aprender de forma divertida a se proteger. Nele você encontra caça-palavras, jogo da memória, dominó, labirinto -- divirta-se e aprenda a usar a Internet com segurança!

Veja também **Guia Internet Segura - para seus filhos**, material complementar com dicas e sugestões para que pais e responsáveis possam orientar seus filhos a usar a Internet com mais segurança e aproveitar ainda mais todas as oportunidades que ela tem a oferecer.

Navegar é preciso, arriscar-se não!

Abaixo você encontra *links* para cada um dos capítulos do **Livro da Cartilha**. Este livro também está disponível nos formatos PDF e ePub.

1. Segurança na Internet

2. Golpes na Internet

3. Ataques na Internet

4. Códigos Maliciosos (*Malware*)

5. *Spam*

6. Outros Riscos

7. Mecanismos de Segurança

8. Contas e Senhas

9. Criptografia

10. Uso Seguro da Internet

11. Privacidade

12. Segurança de Computadores

13. Segurança de Redes

14. Segurança em Dispositivos Móveis

Foi vítima?

- *Sala de Atendimento ao Cidadão do MPF*
  - *http://www.mpf.mp.br/servicos/sac*
- *Polícia Federal*
- *Polícia Civil do DF*
- *Contato direto (Provedor, Banco, responsável, etc)*
- *Ata Notarial*
- *Contate um advogado especialista e/ou perito digital*

Softwares úteis

Qual o melhor antivírus?

- https://www.av-test.org/en/

2FA: Authy e Google Authenticator

Gerenciador de senhas: LastPass e KeePass

Controle Parental: Computador e Celular

Softwares úteis

DuckDuckGo Privacy Essentials

Spybot – Search & Destroy

Eraser

Kleopatra (GPG)

Links úteis

The Top 500 Worst Passwords of All Time	• *http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time*
Check your browser	• *https://browsercheck.qualys.com/*
AmIUnique (ferramentas para privacidade)	• *https://amiunique.org/tools*
Schneier on Security	• *https://www.schneier.com/*

DETALHES

14 de jul. de 2016
qui., 18:24 GMT+02:00

DSC_1234.JPG
8,3 MP 3840 × 2160 1,8 MB

Sony D5833
ƒ/2 1/800 4,6 mm ISO50

Nice, França

http://dfir.com.br