Como aumentar sua segurança no mundo digital

O cenário, a segurança e os riscos

Gilberto Sudre
gilberto@sudre.com.br

GILBERTO SUDRÉ
SEGURANÇA DA INFORMAÇÃO
COMPUTAÇÃO FORENSE

WHOAMI

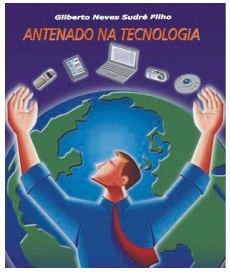
Gilberto Sudré

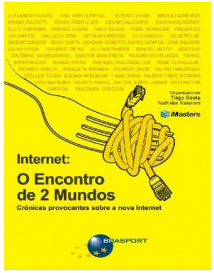
- Professor da **FAESA** – Centro Universitário
- Professor do **IFES** – Instituto Federal do ES
- Coordenador do Laboratório de Pesquisa em Segurança da Informação e Perícia Computacional Forense - **LabSEG**
- Perito e Assistente Técnico em Computação Forense
- Instrutor da **Academia de Polícia Civil do ES** em Computação Forense
- Membro da **APECOF** – Associação Nacional de Peritos em Computação Forense
- Membro da **HTCIA** - High Technology Crime Investigation Association
- Comentarista de Tecnologia da Rádio **CBN Vitória**, **A Gazeta** e **TV Gazeta**

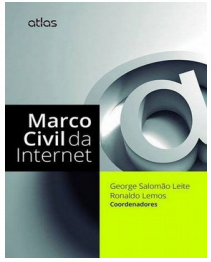
GILBERTO SUDRÉ
SEGURANÇA DA INFORMAÇÃO
COMPUTAÇÃO FORENSE

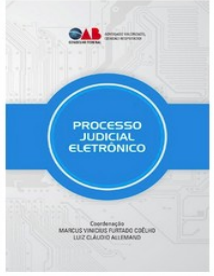
WHOAMI

Gilberto Sudré









GILBERTO SUDRÉ
SEGURANÇA DA INFORMAÇÃO
COMPUTAÇÃO FORENSE

AGENDA

- Nossas informações estão por ai
- Desafios da Segurança Digital
- Cenário
  - Aparelhos inteligentes e a IoT
  - Smartphones e aplicativos
  - Dispositivos “inocentes”
  - Como se defender
- Conclusão

Nossas informações livres por ai...

Expomos voluntariamente nossas informações ...

Expomos voluntariamente nossas informações ...

Um em cada oito recém-nascidos tem conta em redes sociais, diz pesquisa

4% dos bebês têm páginas em redes sociais antes mesmo de nascer.
Um em cada cinco pais publica fotos dos primeiros 15 minutos de vida.

Do G1, em São Paulo

Comente agora | Tweetar 6 | Recomendar 0

Uma pesquisa aponta que um em cada oito recém-nascidos tem conta no **Twitter** ou no **Facebook** criada pelos pais. Cerca de 4% destes tem suas páginas nas redes sociais criadas antes mesmos de eles nascerem.

De acordo com o estudo publicado pela Currys & PC World no Reino Unido, um em cada dez pais compartilham fotos do momento do nascimento dos filhos antes mesmo de os médicos pesarem a criança.

Cerca de 70% dos britânicos tiram fotos de seus filhos recém-nascidos no primeiro dia de vida e um em cada dois pais publicam imagens destes bebês em redes sociais. Um em cada cinco pais publicam imagens nos primeiros 15 minutos de vida dos filhos.

A pesquisa mostra que as redes sociais ajudam os novos pais a enviar notícias aos amigos e parentes. Cerca de 65% deles conversa com um amigo ou parente por meio das fotos do novo bebê antes de encontrar a pessoa de fato.

… e as empresas não cuidam delas.

Netshoes vai ligar para 2 milhões de clientes afetados por vazamento de dados

Por Felipe Ventura
1 ano atrás

NEWS

Em janeiro, o Ministério Público do Distrito Federal e Territórios (MPDFT) alertou sobre "um dos maiores incidentes de segurança registrados no Brasil". Trata-se de uma lista com informações sobre 1.999.704 clientes da Netshoes, incluindo nome completo, e-mail, CPF, data de nascimento e mais.

O MPDFT ameaçou [illegible] fossem avisados s[illegible] telefone.

Banco Inter confirma vazamento de dados e culpa "pessoa autorizada"

Banco diz que a "exposição dos dados foi de baixo impacto"
Imagem: Kacper Pempel/Reuters

Do UOL, em São Paulo
17/08/2018 10h02 | Atualizada em 17/08/2018 11h39

Vazamento da Uber expôs nome, telefone e email de 156 mil usuários brasileiros

Publicado em 13/04/2018 , por **Daniel Camargos**

Brasileiros afetados recebem comunicado da Uber após empresa ser notificada pelo Ministério Público

A Uber começou a notificar os 156 mil brasileiros afetados pelo vazamento dos dados da empresa, em 2016. No email enviado aos usuários a companhia admite que o nome, endereço de email e telefone celular associado a conta foram expostos.

A Uber afirma que os especialistas contratados pela empresa não identificaram indícios de download de histórico de locais de viagens, de números de cartão de crédito e conta bancária e nem das datas de nascimento.

31/08/2018 às 14h50

C&A é alvo de hackers no Brasil, com vazamento de dados de clientes

Por **Cibelle Bouças | Valor**

SÃO PAULO - Na madrugada de quinta-feira (30), a varejista de moda C&A do [illegible] invadiram o seu sistema de vale-

INFORME AQUI

Vazamento da Equifax compromete dados de 143 milhões de clientes

19 de setembro de 2017 2 minutos de leitura

Em maio, a Equifax, uma das maiores agências de monitoramento de crédito dos Estados Unidos, teve os dados confidenciais de mais de 143 milhões de clientes no país comprometidos, em um dos maiores

Por [illegible]

Comp[illegible]

CASO CAMBRIDGE ANALYTICA ›

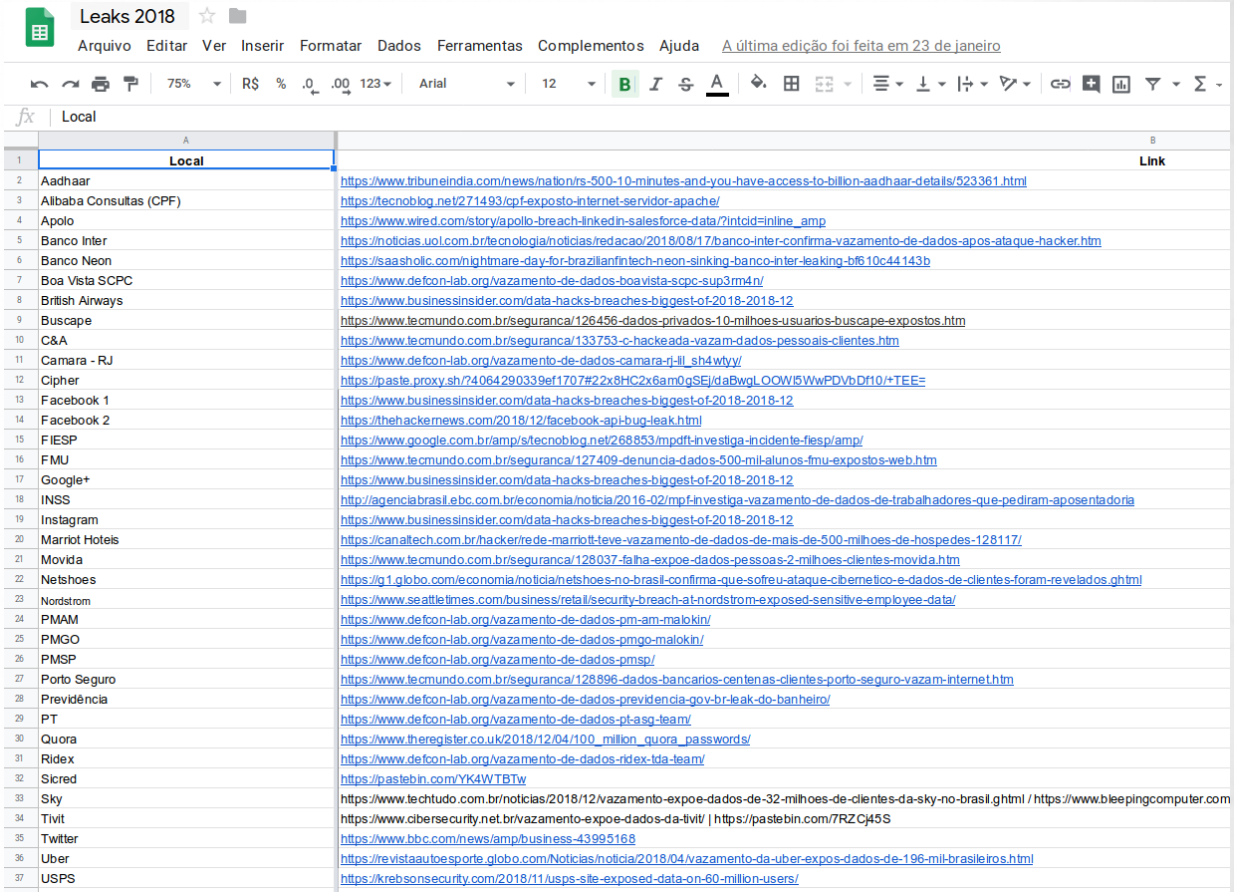
Vazamento de dados do Facebook causa tempestade política mundial

Autoridades dos EUA e Reino Unido exigem que Zuckerberg dê explicações depois da revelação de que uma consultoria eleitoral manipulou informações de 50 milhões de usuários da rede social

PABLO DE LLANO | ÁLVARO SÁNCHEZ
Miami / Bruxelas - 20 MAR 2018 - 17:35 CET

… e as empresas não cuidam delas.

... e as empresas não cuidam delas.

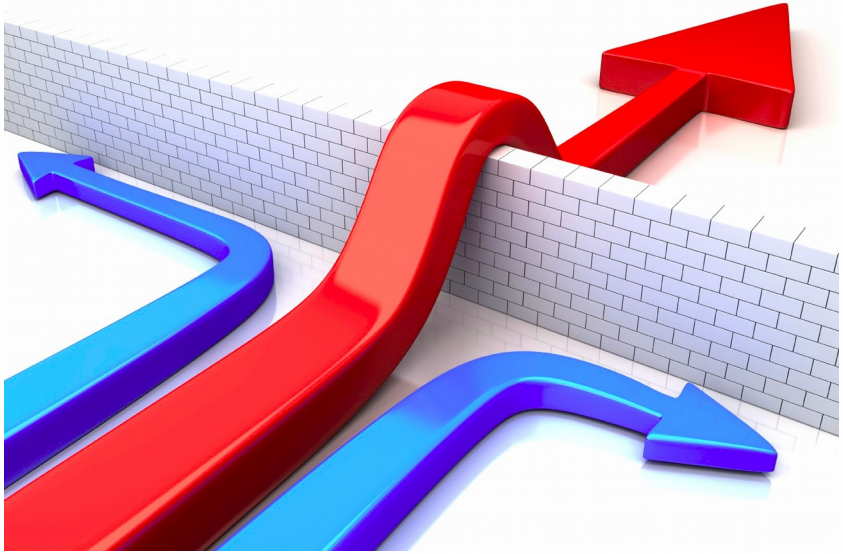


Leaks 2018

Arquivo Editar Ver Inserir Formatar Dados Ferramentas Complementos Ajuda A última edição foi feita em 23 de janeiro

Local

	Local	Link
2	Aadhaar	https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html
3	Alibaba Consultas (CPF)	https://tecnoblog.net/271493/cpf-exposto-internet-servidor-apache/
4	Apolo	https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/?intcid=inline_amp
5	Banco Inter	https://noticias.uol.com.br/tecnologia/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm
6	Banco Neon	https://saasholic.com/nightmare-day-for-brazilianfintech-neon-sinking-banco-inter-leaking-bf610c44143b
7	Boa Vista SCPC	https://www.defcon-lab.org/vazamento-de-dados-boavista-scpc-sup3rm4n/
8	British Airways	https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
9	Buscape	https://www.tecmundo.com.br/seguranca/126456-dados-privados-10-milhoes-usuarios-buscape-expostos.htm
10	C&A	https://www.tecmundo.com.br/seguranca/133753-c-hackeada-vazam-dados-pessoais-clientes.htm
11	Camara - RJ	https://www.defcon-lab.org/vazamento-de-dados-camara-rj-lil_sh4wtyy/
12	Cipher	https://paste.proxy.sh/?4064290339ef1707#22x8HC2x6am0gSEj/daBwgLOOWI5WwPDVbDf10/+TEE=
13	Facebook 1	https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
14	Facebook 2	https://thehackernews.com/2018/12/facebook-api-bug-leak.html
15	FIESP	https://www.google.com.br/amp/s/tecnoblog.net/268853/mpdft-investiga-incidente-fiesp/amp/
16	FMU	https://www.tecmundo.com.br/seguranca/127409-denuncia-dados-500-mil-alunos-fmu-expostos-web.htm
17	Google+	https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
18	INSS	http://agenciabrasil.ebc.com.br/economia/noticia/2016-02/mpf-investiga-vazamento-de-dados-de-trabalhadores-que-pediram-aposentadoria
19	Instagram	https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12
20	Marriot Hoteis	https://canaltech.com.br/hacker/rede-marriott-teve-vazamento-de-dados-de-mais-de-500-milhoes-de-hospedes-128117/
21	Movida	https://www.tecmundo.com.br/seguranca/128037-falha-expoe-dados-pessoas-2-milhoes-clientes-movida.htm
22	Netshoes	https://g1.globo.com/economia/noticia/netshoes-no-brasil-confirma-que-sofreu-ataque-cibernetico-e-dados-de-clientes-foram-revelados.ghtml
23	Nordstrom	https://www.seattletimes.com/business/retail/security-breach-at-nordstrom-exposed-sensitive-employee-data/
24	PMAM	https://www.defcon-lab.org/vazamento-de-dados-pm-am-malokin/
25	PMGO	https://www.defcon-lab.org/vazamento-de-dados-pmgo-malokin/
26	PMSP	https://www.defcon-lab.org/vazamento-de-dados-pmsp/
27	Porto Seguro	https://www.tecmundo.com.br/seguranca/128896-dados-bancarios-centenas-clientes-porto-seguro-vazam-internet.htm
28	Previdência	https://www.defcon-lab.org/vazamento-de-dados-previdencia-gov-br-leak-do-banheiro/
29	PT	https://www.defcon-lab.org/vazamento-de-dados-pt-asg-team/
30	Quora	https://www.theregister.co.uk/2018/12/04/100_million_quora_passwords/
31	Ridex	https://www.defcon-lab.org/vazamento-de-dados-ridex-tda-team/
32	Sicred	https://pastebin.com/YK4WTBTw
33	Sky	https://www.techtudo.com.br/noticias/2018/12/vazamento-expoe-dados-de-32-milhoes-de-clientes-da-sky-no-brasil.ghtml / https://www.bleepingcomputer.com
34	Tivit	https://www.cibersecurity.net.br/vazamento-expoe-dados-da-tivit/ | https://pastebin.com/7RZCj45S
35	Twitter	https://www.bbc.com/news/amp/business-43995168
36	Uber	https://revistaautoesporte.globo.com/Noticias/noticia/2018/04/vazamento-da-uber-expos-dados-de-196-mil-brasileiros.html
37	USPS	https://krebsonsecurity.com/2018/11/usps-site-exposed-data-on-60-million-users/



Desafios da Segurança Digital

Desafios da Segurança Digital

- **Globalização das insegurança**
  - Novas Ameaças, Vulnerabilidades e Riscos

- **Globalização dos Alvos**
  - Pessoas, Empresas e **Governos**
  - Ataques a infra estruturas críticas

Desafios da Segurança Digital

The Cost of Cybercrime

By Grant Gross
Technology Reporter

Most people paying attention would expect that the cost of cybercrime has gone up in recent years. But a new report has put a number on it: Worldwide cybercrime costs an estimated $600 billion USD a year.

That's up from $500 billion USD in 2014, the last time security vendor McAfee and think tank the Center for Strategic and International Studies released a similar study. The new estimate amounts to 0.8 percent of global GDP, up from 0.7 percent in 2014.

"Cybercrime is relentless, undiminished, and unlikely to stop," writes report author James Lewis, senior vice president at CSIS. "It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low."

EXECUTIVE SUMMARY

The Economic Impact of Cybercrime—No Slowing Down

Cybercrime now costs the world almost $600 billion, or 0.8 percent of global GDP, according to a new report by the Center for Strategic and International Studies (CSIS) and McAfee. Scheduled for release February 21, "The Economic Impact of Cybercrime: No Slowing Down" updates the popular 2014 report, which put global losses at close to $500 billion, or 0.7% of global income.

To put the latest statistic in perspective, it amounts to more than the income of almost all but a few countries. When you look at the cost of cybercrime in relation to the worldwide internet economy—$4.2 trillion in 2016—cybercrime can be viewed as a 14% tax on growth[1].

As crimes with global impact go, cybercrime ranks third, behind government corruption and narcotics as a global economic scourge[2], and here's why:

- **Low-risk to high payoff:** The probability of getting arrested or going to jail is low. Not one of the perpetrators of the biggest headline-grabbing breaches has been prosecuted. Law enforcement agencies are stepping up their efforts, but many cybercriminals operate outside of their jurisdictions.

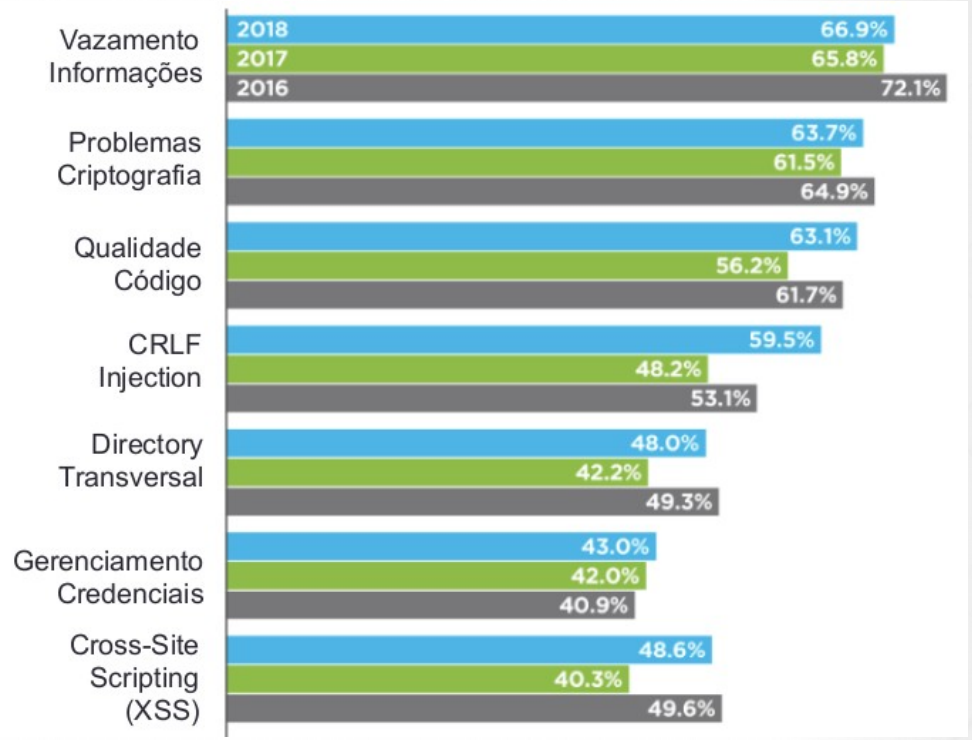
The report attributes the $100 billion growth in cybercrime to cybercriminals quickly adopting new

Desafios da Segurança Digital

- **O ambiente de TI está cada vez mais complexo**
  - Novas tecnologias
  - Muitos aplicativos e protocolos
  - Interatividade por vários meios e canais de comunicação
  - A informação está em muitos locais

Desafios da Segurança Digital

- ✔ **Problemas mais comuns em relação a Segurança Digital**



Fonte: Veracode CA

Desafios da Segurança Digital

- **As ações de segurança precisam estar integradas com a legislação e regulamentação**
  - Responsabilidade Civil dos administradores e técnicos
  - Atendimento a Agências Reguladoras
  - Gestão de Segurança através de normas e padrões
  - Marco Civil da Internet, LDPGp, GDPR....

Desafios da Segurança Digital

- **A segurança da informação não é só em computadores**
  - Sistemas de Telecomunicações
  - Informações em Papel e outros suportes
  - Roubo de equipamentos
  - Descarte de equipamentos e acessórios

Desafios da Segurança Digital

- **O valor financeiro da rede está aumentando**
  - Transações financeiras pela Internet
  - Transações financeiras em sistemas internos
  - Relacionamento pessoal
  - Armazenamento de informações de valor

Desafios da Segurança Digital

- **O crime organizado tem aumentado sua atividade no meio eletrônico**
  - Para usar novas tecnologias em crimes convencionais
  - Para novos crimes tecnológicos
  - O conhecimento de sobre com realizar os ataques está disponível gratuitamente

Desafios da Segurança Digital

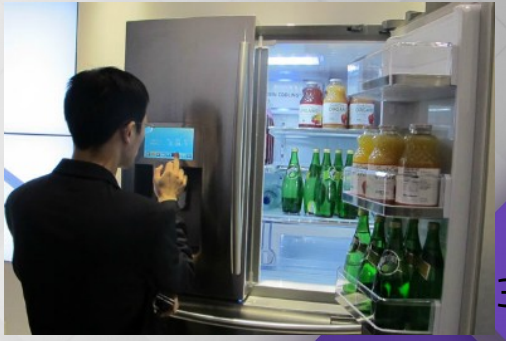
- **Crimes são transnacionais**
  - Dificuldade de investigação
  - Cooperação com outras Polícias
  - Paraísos na Internet sem controle de hospedagem
  - IPv6

E continuamos a cometer os mesmos erros...

- **Anexos continuam funcionando para infectar usuários**
  - Agora com mais abrangência
    - E-mail, Whatsapp, Telegram e outros
  - 23% dos destinatários de phishing abrem as mensagens
  - 11% deles clicam nos anexos
  - 50% abrem os e-mails na primeira hora em ele chega

Aparelhos inteligentes (IoT) e seus riscos

Eles já estão entre nós..



.. e em grande quantidade.

Número de conexões IoT já supera as de smartphones nos Estados Unidos

Chetan Sharma Consulting estima 1,4 milhão de carros conectados entre abril e junho, contra 1,2 milhão de telefones

Riscos da IoT

Tecnologia

Segurança da Internet das Coisas é uma "bomba-relógio"

Redes baseadas em sensores pioram a proteção dos sistemas de informação devido à velocidade da evolução tecnológica que as suporta

Da Redação, com IDG News Service
Publicada em 13 de maio de 2015 às 08h21

E-mail Imprima Erros? a a a

Tweet

Riscos da IoT a sua privacidade

- **TV Samsung:**
  - Wireless
  - Comando por Voz
  - Acesso a Internet
  - Reconhecimento Facial
  - Webchat
  - Compras on-line
- Mas a Samsung avisa...

Riscos da IoT a sua privacidade

TECNOLOGIA

Samsung adverte: Cuidado com o que você diz em frente a sua TV inteligente

Fabricante alerta consumidores de que televisão pode gravar conversas próximas e transmitir diálogos a terceiros

POR O GLOBO

09/02/2015 13:06 / atualizado 09/02/2015 13:58

Riscos da IoT a sua tranquilidade

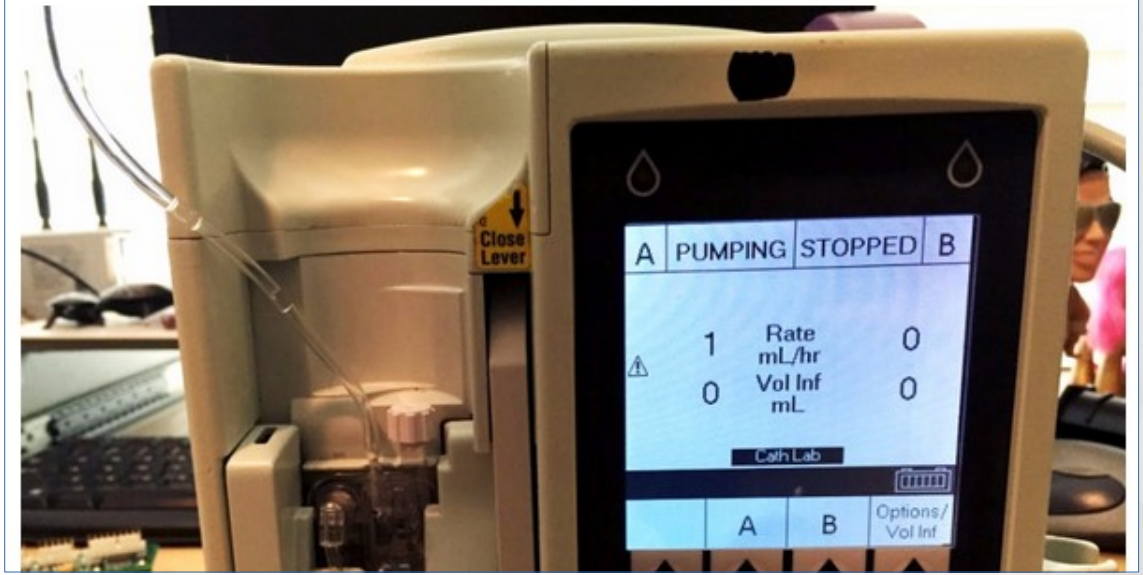
Riscos da IoT a sua saúde

NOTÍCIAS SEGURANÇA

Hackers podem alterar remotamente bombas de remédios em hospitais, diz pesquisador

Gabriel Garcia, da INFO

0 08/06/2015 09h48



Riscos da IoT a sua saúde

Segurança

Bombas de insulina da J&J estão vulneráveis a ataques remotos

IDG News Service 05/10/2016 - 15h20

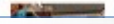
Brechas encontradas por pesquisador expõe a necessidade de reforçar a segurança de dispositivos médicos

ÚLTIMAS NOTÍCIAS


Venda de smartphones melhora no Brasil, mas mantém queda em 2016


Lenovo pode comprar a divisão de PCs da Fujitsu


Tinta para impressora 3D pode ser usada para produzir ossos sintéticos


Avião é evacuado nos EUA após

Riscos da IoT a sua saúde

Segurança

Bombas de insulina da J&J estão vulneráveis a ataques remotos

IDG News Service 05/10/2016 - 15h20

Brechas encontradas por pesquisador expõe a necessidade de reforçar a

E o fabricante.....


phones melhora no
tém queda em 2016


Lenovo pode comprar a divisão de PCs da Fujitsu


Tinta para impressora 3D pode ser usada para produzir ossos sintéticos


Avião é evacuado nos EUA após

Riscos da IoT: A saúde

- E o fabricante...

> "A probabilidade de um acesso não autorizado no OneTouch Ping é extremamente baixa", disse a companhia, em comunicado enviado a médicos na segunda-feira e a 114 mil pacientes que usam o dispositivo nos Estados Unidos e Canadá.

> "Precisaria de expertise técnica, equipamento sofisticado e proximidade com a bomba, já que o sistema OneTouch Ping não está conectado à Internet ou a qualquer rede externa", afirmou a empresa.

Riscos da IoT ao seu sigilo

SmartWatches e pulseiras fitness podem revelar suas senhas com facilidade

06 de julho de 2016 5

Os dispositivos wearable de pulso podem definitivamente **trair os seus donos** em algum momento. Um novo estudo, ameaçadoramente intitulado "*Amigo ou inimigo? Seus dispositivos Wearable revelam seu PIN pessoal*", revela que é surpreendentemente simples descobrir o PIN ou palavra-chave de um usuário, através de engenharia reversa dos dados capturados pelo sensor de movimento de um SmartWatch ou monitor de exercícios físicos.

No estudo, uma equipe de pesquisadores da Universidade de Binghamton e do Instituto Stevens de Tecnologia descrevem um método fácil que supostamente permite a um invasor adivinhar senha de um alvo, com cerca de **80% de precisão apenas na primeira tentativa.** Embora o documento não cite os dispositivos específicos que podem proporcionar esse tipo de ataque, ele destaca que vários modelos gravam os movimentos de sua mão com detalhes suficientes para identificar com precisão quais são as teclas pressionadas pela mão que utiliza o wearable.

Riscos da IoT a sua segurança

ESTADÃO ›

Annotations

Veículos autônomos são alvo de ataques nos EUA

JANUARY 25, 2019

CHANDLER, ARIZONA - O agressor saiu de um parque certo dia em outubro, avançando contra o alvo, parado num cruzamento: uma van autônoma operada pela Waymo, a empresa de veículos sem motorista que nasceu do Google. Ele furou um dos pneus e desapareceu nas ruas do bairro.

O episódio fez parte de mais de duas dúzias de ataques contra veículos sem motorista cometidos nos últimos dois anos em Chandler, uma cidade próxima de Phoenix onde a Waymo começou a testar suas vans em 2017. A cidade teve a oportunidade de conhecer antes das demais as reservas do público em relação à ascensão da inteligência artificial, com queixas a

INSIGHTTRADE.COM.BR ›

Annotations

Veículos autônomos têm pelo menos 50 pontos de ciberataque, afirma Indra

DECEMBER 04, 2018

Companhia trabalha no desenvolvimento de soluções para proteger novos veículos contra o crime virtual e proporcionar uma experiência satisfatória a empresas e usuários

A discussão sobre o avanço dos veículos autônomos ganha cada vez mais espaço no cenário mundial. Recentemente, a Alphabet informou que

Riscos da IoT a sua casa

become a supporter

theguardian

news / opinion / sport / arts / life

Roomba maker may share maps of users' homes with Google, Amazon or Apple

iRobot's chief executive says company could share or sell maps of robot vacuum users' homes to US tech firms as part of smart home and profit push

iRobot's Roomba robotic vacuum cleaners could soon be sharing the maps of users' homes they make as they clean with Amazon, Apple or Google, among others. Photograph: Reuters

O aspirador-robô Roomba foi hackeado para gritar e xingar. Confira!

Redação Olhar Digital 09/05/2019 17h34

Compartilhe com seus seguidores

A A A

O Roomba tem uma reação muito humana - e bem hilária - quando colide com móveis e paredes

Parafraseando velho ditado da internet: "Municípios têm limite. A zoeira não". Pensando nisso, um youtuber resolveu hackear o popular aspitador-robô Roomba e dar um, digamos, upgrade nele. Em outras palavras, ele criou uma versão do Roomba que esperneia e xinga ao colidir com algum móvel — como fazemos quando batemos o dedinho

Smartphones e seus aplicativos

Smartphones e seus aplicativos

The Hacker News™
Security in a serious way

New Exploit to 'Hack Android Phones Remotely' threatens Millions of Devices

Wednesday, March 16, 2016 Swati Khandelwal

The Hacker News™
Security in a serious way

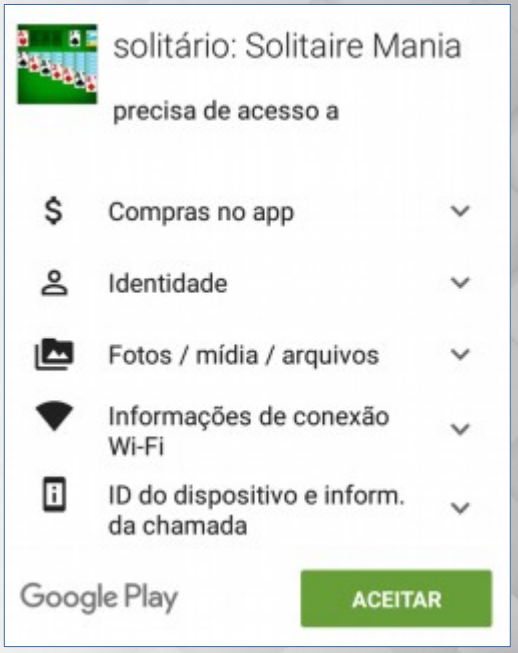
iPhone Apps With Camera Permissions Can Secretly Take Your Photos Without You Noticing

Sunday, October 29, 2017 Mohit Kumar

Are you a proud iPhone owner? If yes, this could freak you up. Trust me!

Your iPhone has a serious privacy concern that allows iOS app developers to take your photographs and record your live video using both front and back camera—all without any notification or your consent.

Smartphones e seus aplicativos



Outros dispositivos “inocentes”

Outros dispositivos “inocentes”

Como se defender?

Como se defender?

- Técnicas
  - Criptografia
  - Desenvolvimento seguro de código
  - Autenticação
  - Atualização dos softwares
  - Isolamento de tráfego
  - A segurança deve estar embutida nos sistemas e não uma camada extra

Como se defender?

- Politicas
  - Legislação e punição severa para o uso indevido de informações
  - Controle do que está sendo feito com nossas informações

- Comportamentais
  - Informação, esclarecimento e educação para pessoas não técnicas
  - Acabar com o conformismo: “Isto é normal” ou “Eu não tenho nada a esconder”
  - Valorização da privacidade

Conclusão

Conclusão

- ✔ Pensamento Neurótico?

Conclusão

- ✔ Pensamento Neurótico?

“No mundo da Tecnologia só os neuróticos sobrevivem.”

Paul Otellini, CEO da Intel

Conclusão

- As ameaças continuarão a evoluir
- Continuaremos a tratar a segurança de forma reativa, apagando incêndio?
- Precisamos repensar a Segurança da Informação
  - Conhecer as vulnerabilidades e ameaças
  - Planejamento e normalização
  - Infraestrutura segura
  - Auditoria
  - Educação e Treinamento

Obrigado

 **gilbertosudretecnologia**

 **gilbertosudre**

 **gilbertosudre**

 **gilberto@sudre.com.br**

 **gscomputacaoforense.com.br**