



Ensino a distância
Aprendizado Contínuo
Liberdade
Colaborativismo

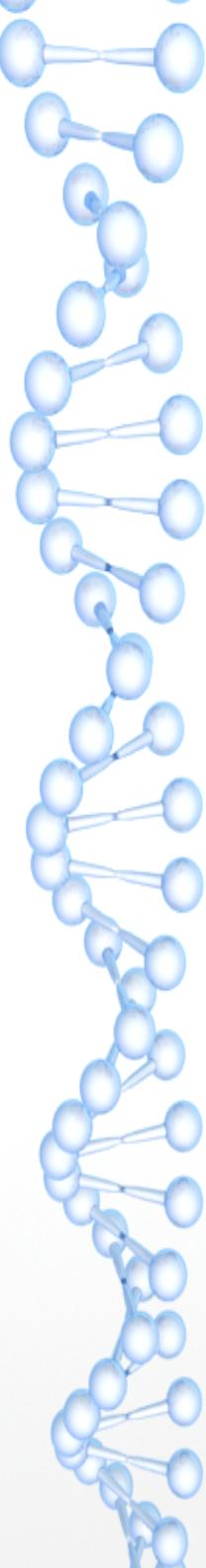
- * **Vídeo aulas**
- * **Documentações**
- * **Dicas**



youtube.com/projetoroot

- diegocosta@projetoroot.com.br
- www.projetoroot.com.br
- youtube.com/projetoroot
- facebook.com/projetoroot
- wiki.projetoroot.com.br

•
Diego Costa
CEO – Projeto Root



Neivia Justa • 2º

LinkedIn Top Voice, Senior Communication, Institutional...

3 d

"Mãe, preciso de um RG falso para ir à festa do 3º ano."

- Como assim, filha?

"Todo mundo tem um RG falso para ir às festas onde tem bebida, mãe."

- Sério? Mas isso é crime, previsto em lei, filha. Como é possível os pais dos seus colegas deixarem eles terem um RG falso?

"Não sei, mãe. Só sei que todo mundo tem."

- Você não terá. Você não é todo mundo. E eu vou levar esse assunto à coordenação da sua escola.

Essa foi uma conversa que tive com minha filha de 15 anos, que está no segundo ano do ensino médio.

Fiquei horrorizada com o pedido e, ainda mais, ao descobrir a "naturalização" do tema entre adolescentes. Também descobri, numa pesquisa básica na internet, inúmeros "serviços" e "tutoriais" de falsificação de RG.

É assim que defendemos a ética e o combate à corrupção?

Fazendo vista grossa e deixando nossos filhos alimentarem essa "indústria" do crime que produz RGs falsos para menores de idade?

Que exemplos de pais somos nós?

Que filhos vamos deixar para o mundo?

A **#mudança** tem que começar em nós, na maneira como educamos nossas crianças.

#JustaCausa

- Especialista em Segurança da Informação – Faculdade de Tecnologia SENAC – Porto Alegre - RS
- Tecnólogo em Redes de Computadores – Faculdade de Tecnologia SENAC – Pelotas - RS
- Criador de conteúdos online na área de tecnologia e idealizador do canal no Youtube Projeto Root
- Consultor e Analista de Segurança da Informação
- Professor Faculdade de Tecnologia Senac – Pós-Graduação em Segurança da Informação.

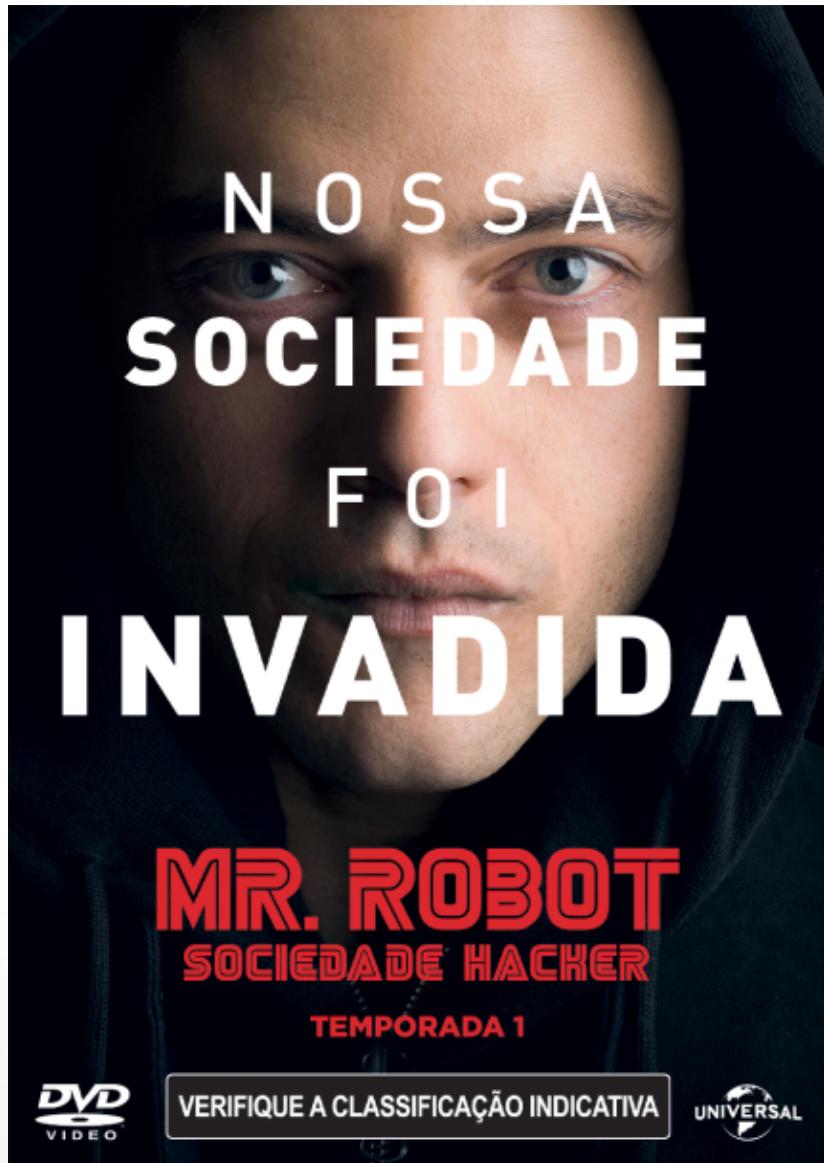


(IN)Segurança na INternet



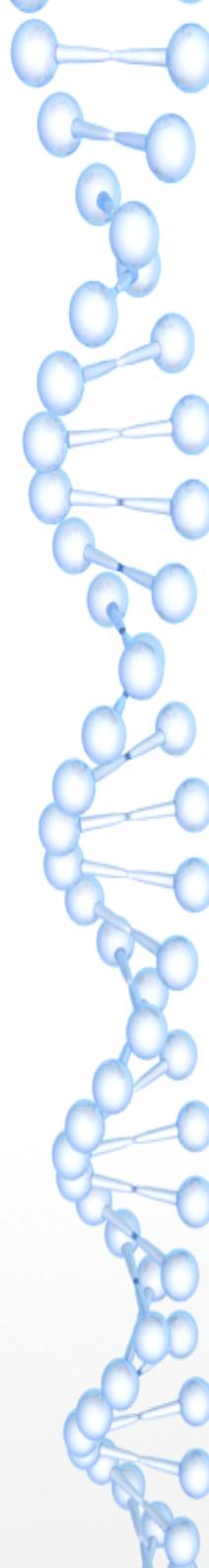
- O que faço na internet ?
- Quem está lá ... ?
- Quais os riscos de uma navegação descuidada?
- A empresa que trabalho pode sofrer danos com o meu descuido?
- Posso mudar este cenário?

Ficção na Realidade ou Realidade na Ficção?



Minha casa, sua casa?



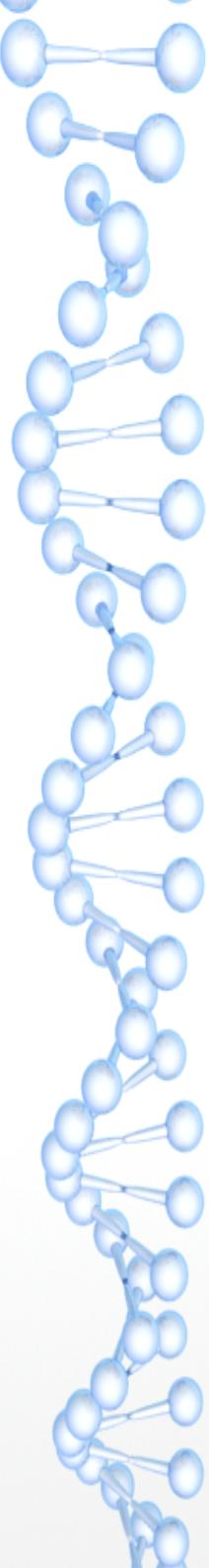


Você sabe como a internet funciona?



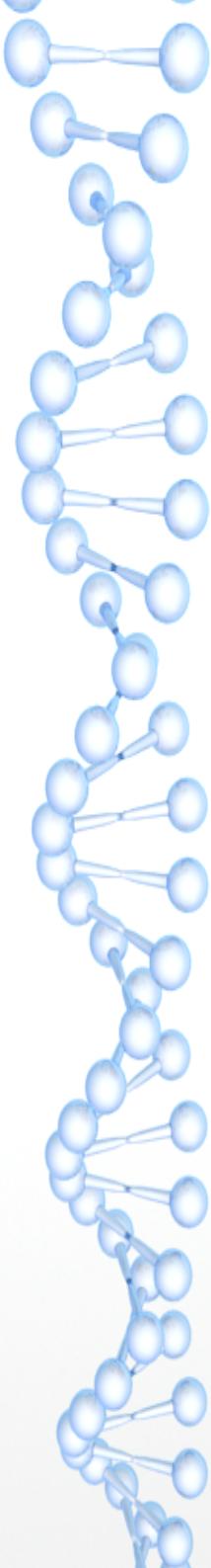
Será mesmo que ela é como você imagina?





Perigos na navegação

- * Invasão de computadores e dispositivos informáticos;
- * Perdas e/ou **vazamento de dados sensíveis** ;
- * Extorsão/Golpes;
- * Fake News;
- * Aproveitamento/Uso de informações privilegiadas;
- * Prejuízos inestimáveis ao afetado.



Mas isso todo mundo sabe, né?

Vivemos em um mundo pós Edward Snowden

Sabemos ou deveríamos saber que **empresas** como:

- * Facebook
- * Google
- * Microsoft
- * Yahoo
- * etc...

Fazem **bilhões** de dólares em lucro com:

- * Nossos perfis de navegação
- * Nossas orientações (religiosas, políticas, sexual, ideológicas,etc..)
- * Nossas compras (online e offline)
- * Nossas localizações (Check-IN, maps, marcações)
- * etc...



Mais 5



Atividade na linha do tempo



Você andou 11 km este mês



Você passou mais de 60 horas em um veículo este mês



Estatísticas de toda a sua linha do tempo

Mais 379.356 km até a Lua



2

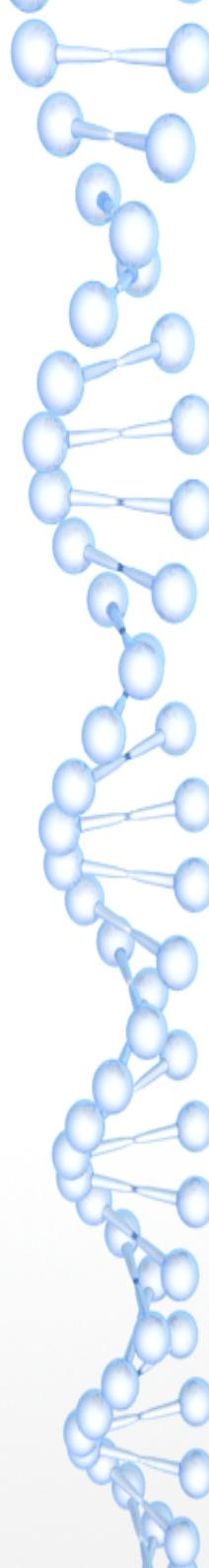
cidades visitadas no total



17

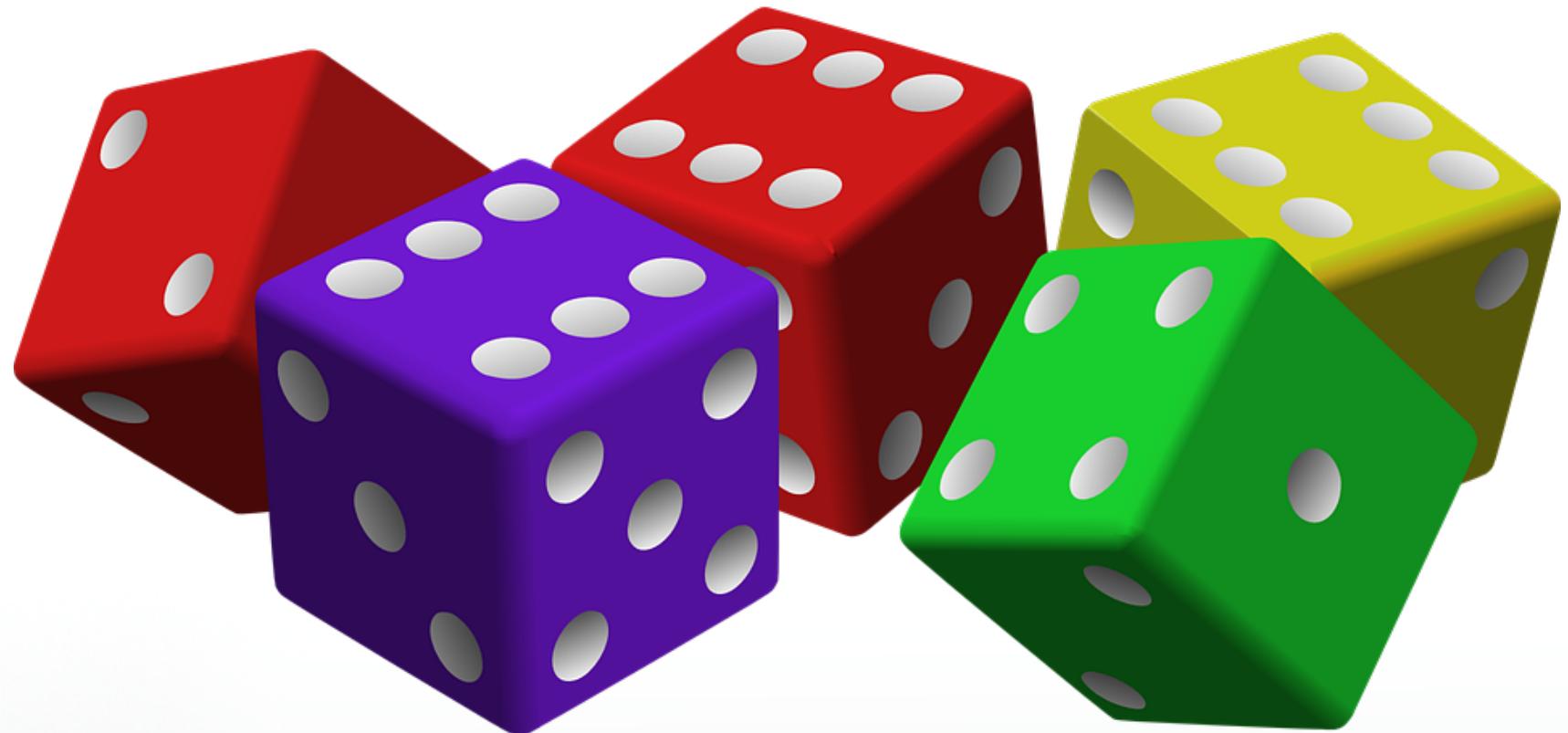
lugares visitados no total





Mas como isso é possível?

Apenas com o maior bem (ativo) que você tem.



“Dados” - Quanto criamos?

Estima-se que uma pessoa (normal) gere 1TB de informação sensível por ano.



Novo - 191 vendidos

Hd 1tb Tera Western Digital Blue Sata 7200 Wd 3.5

5 ⭐️ 303 opiniões

R\$ 268

12x R\$ 22³³ sem juros



Mais informações

Frete grátis

Chegará entre os dias 9 e 13 de maio
Benefício Mercado Pontos

[Ver mais opções](#)

Devolução grátis

Você tem 15 dias a partir do recebimento

Quantidade: 1 unidade ▾ (81 disponíveis)





Mas como? eu não ...

Será que não?



CURTIR

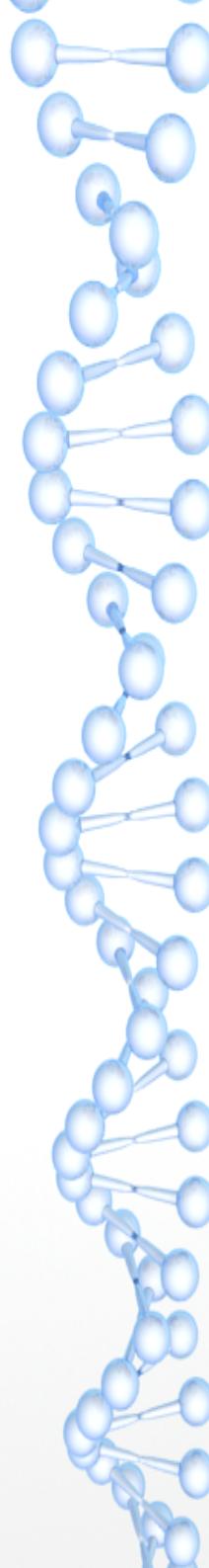


COMENTAR



COMPARTILHAR

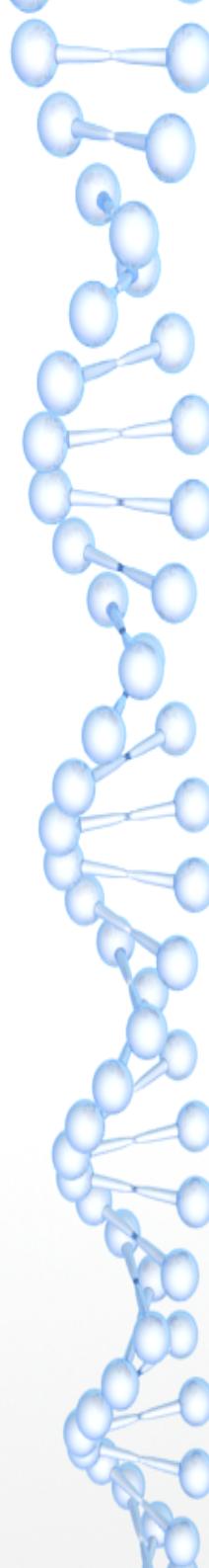




Mas como? eu não ...

Será que não?



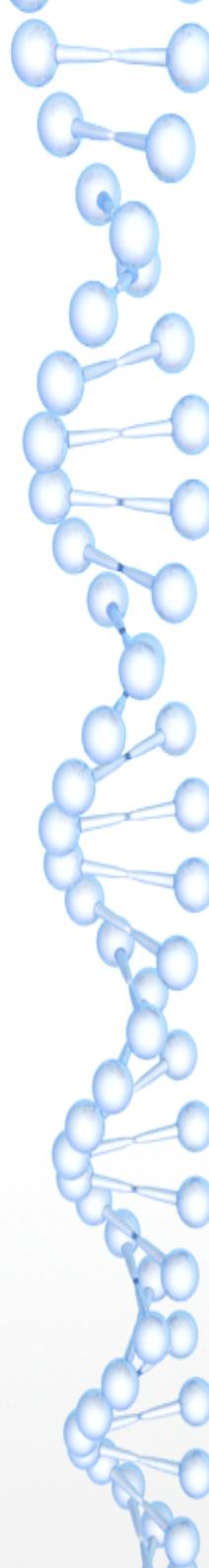


Mas como? eu não ...

Será que não?

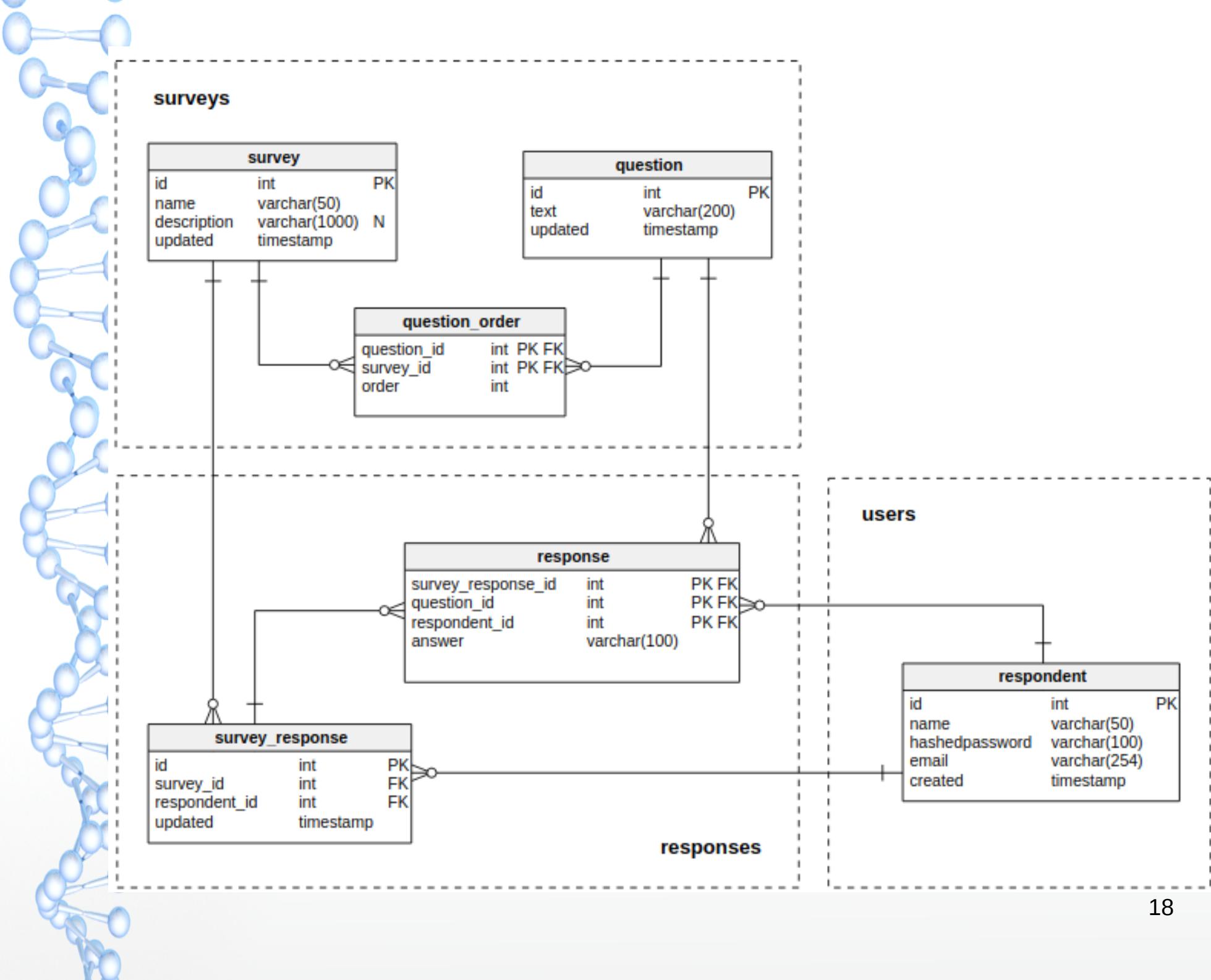


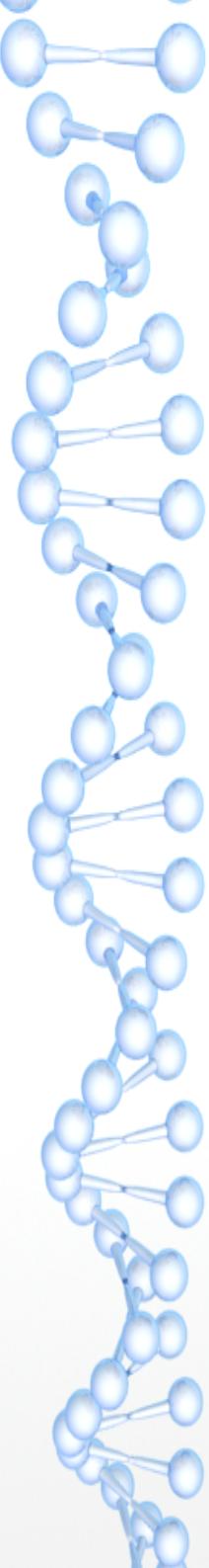
Alô, não tem
nenhum joão
aqui, ligou para o
número errado.



Mas como? eu não ...







Não, comigo não ...

Tem certeza?





Tainara Hirsch ▶ Vagas Abertas Online

9 min ·

...

O SENAC está abrindo novas turmas para seus cursos gratuitos. Confira os cursos e se inscreva! Comentar "EU QUERO" para receber o link de inscrição!
Não corra atrás de alguém que não dá um passo por você.



CURSOS TÉCNICOS GRATUITOS



Ambiente	CURSOS TÉCNICOS EAD	HORÁRIO	VAGAS
Beleza	TÉCNICO EM ENFERMAGEM	13hrs até 17hrs	25
Comércio	TÉCNICO EM RADIOLÓGIA	19hrs até 22hrs	30
Design	TÉCNICO EM ADMINISTRAÇÃO	08hrs até 11hrs	80
Gestão	TÉCNICO EM FARMÁCIA	13hrs até 17hrs	60
Informática	TÉCNICO EM MASSOTERAPIA	19hrs até 22hrs	25
Moda	TÉCNICO EM PODOLOGIA	08hrs até 11hrs	28
Saúde	TÉCNICO EM FINANCIAS	19hrs até 22hrs	22
Segurança	TÉCNICO EM PUBLICIDADE	08hrs até 11hrs	54
Turismo	TÉCNICO EM RADIOLÓGIA	13hrs até 17hrs	35
	TÉCNICO EM RECURSOS HUMANOS	19hrs até 22hrs	30
	TÉCNICO EM SEGURANÇA NO TRABALHO	08hrs até 11hrs	54

3

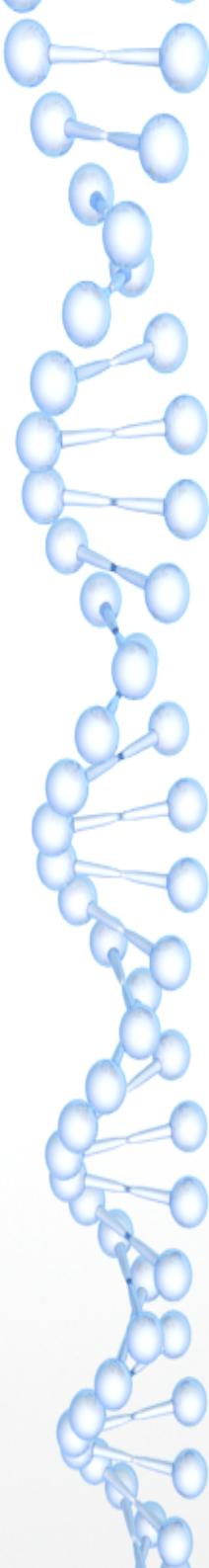
7 comentários

SENAC PRONATEC 2019 → Cursos Gratuitos PRONATEC, Inscrições

<https://senac2018.com/senac-pronatec-2019/> ▾

★★★★★ Avaliação: 4,6 - 26 votos

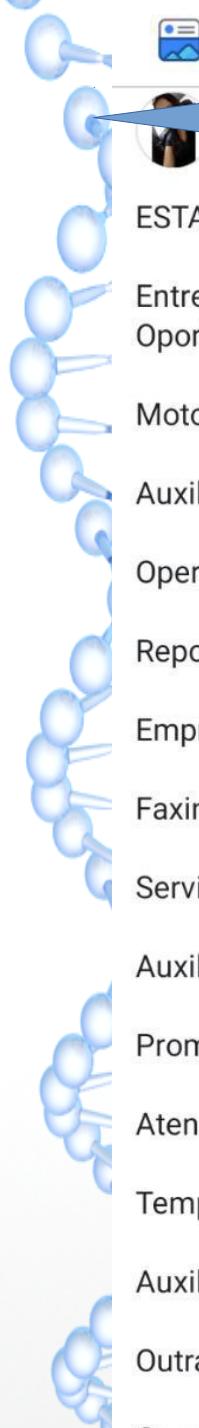
O SENAC PRONATEC 2019 permite que você inicie o ano estudando de forma gratuita. O projeto tem parceria com o Governo Federal e auxilia futuros ...



Não se deixe enganar: confira sempre nossa programação aqui ou no site www.senacrs.com.br/riogrande. #SenacRioGrande 😊

FAKE NEWS

Algumas páginas e sites estão divulgando informações falsas e/ou incorretas sobre os nossos cursos. Lembre-se: para qualquer informação sobre o Senac, acesse os nossos sites ou os perfis oficiais nas redes sociais.



Vendas Rio Grande 

Há 12 minutos 

ESTAMOS CONTRATANDO:

Entrevistas ainda nesta semana!!!
Oportunidades disponíveis:

Motorista D (R\$ 1874,46)

Auxiliar de Carga e Descarga (R\$ 1.052,00)

Operador de caixa (R\$ 1030,00)

Repositor (R\$ 1.390,00)

Empregada Doméstica (R\$1200,00)

Faxineiro (R\$ 1.138,94)

Serviços Gerais (R\$ 1150,00)

Auxiliar de Limpeza (R\$1500,00)

Promotor de Merchandising (R\$1.200,00)

Atendente Cacau Show (R\$ 1200,00)

Temporários dia dos namorados (R\$ 1400,00)

Auxiliar de Produção (R\$ 1.540,00)

Outras vagas...

Caso tenha interesse entre em contato via whatsapp:
(21) 97222-7862, dizendo a vaga que pretende .

 Vendas Rio Grande 

1 h 

CANDIDATE-SE  <http://bit.ly/2YBlfe4>

R\$ 125

Brasil

Bom para todos interessados!!

EMPRESAS CONTRATANDO!!!

Menor Aprendiz Auxiliar (998,00)
Auxiliar de Creche
Atendente para loja de açaí (1.385,00)
Serviços Gerais (FEMININO)
Atendente (Quiosque Infantil)
Auxiliar de Produção de Embalagens
Auxiliar de Serviços Gerais (HOSPITALAR)
Degustadora (Produtos Naturais)
Ajudante de Mecânico (1.551,00)
Operador de Monitoramento
Assistente de Loja (14:30h as 22:30h)
Empacotador de Loja
Caseiro (1.500,00)
Entre outras...

Envie seu currículo

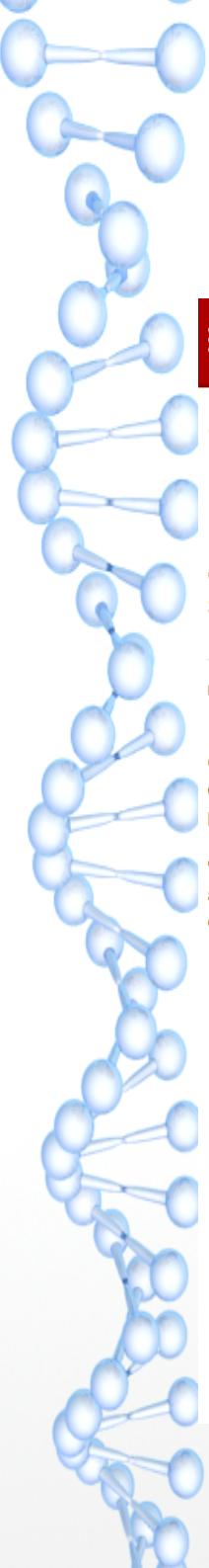
Interessados(as) C O N F I R M E M com " OK " + vaga desejada!

 1

 Enviar mensagem ao vendedor

4 comentários

Mas quem é esse tal Snowden?



MENU | **G1** **MUNDO**

17/03/2016 17h34 - Atualizado em 17/03/2016 18h18

Edward Snowden cita grampo de Dilma no Twitter

'Dilma ainda faz chamadas não criptografadas', diz ex-analista da NSA. Snowden cita caso de 2013 quando presidente foi alvo de escuta dos EUA.

Do G1, em São Paulo

O ex-consultor da Agência de Segurança Nacional (NSA) Edward Snowden postou nesta quinta-feira (17) no Twitter uma mensagem em que cita o grampo telefônico envolvendo o ex-presidente Luiz Inácio Lula da Silva e a presidente Dilma Rousseff.

"Going dark" é um conto de fadas: três anos após as manchetes de escuta de @dilmabr ela ainda está fazendo chamadas não criptografadas", diz a mensagem acompanhada de uma colagem de manchetes da imprensa americana de setembro de 2013 e desta quinta.

 **Edward Snowden** 
@Snowden



"Going dark" is a fairy tale: 3 years after @dilmabr wiretap headlines, she's still making unencrypted calls. [#opsec](#)

AP September 1, 2013, 11:43 PM

Report: NSA spied on Brazilian, Mexican presidents

Tweeted by CNN Internatio... Mar 17, 2016

BBC | **Menu**

NEWS | BRASIL

Notícias | Brasil | Internacional | Economia | Saúde | Ciência | Tecnologia | Aprenda Inglês

EUA espionaram Petrobras, dizem papéis vazados por Snowden

08 setembro 2013

    Compartilhar

Novos documentos da Agência de Segurança Nacional dos Estados Unidos (NSA) vazados pelo ex-analista da agência Edward Snowden indicam que a Petrobras também teria sido espionada pelos americanos.

A informação vem uma semana após notícias de que a presidente do Brasil, Dilma Rousseff, teria sido espionada pela agência.

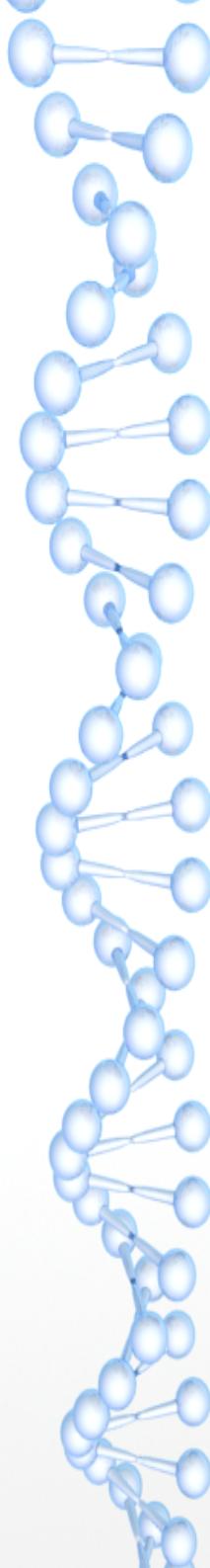
O teor dos documentos sobre a Petrobras foi revelado em reportagem do programa *Fantástico*, da TV Globo.

Segundo a reportagem, a tecnologia envolvendo a exploração em alta profundidade na camada pré-sal poderia ter sido o alvo da espionagem. Consultada, a Petrobras disse que não fará comentários.

Nome da Petrobrás aparece em treinamento sobre como invadir redes de dado privadas

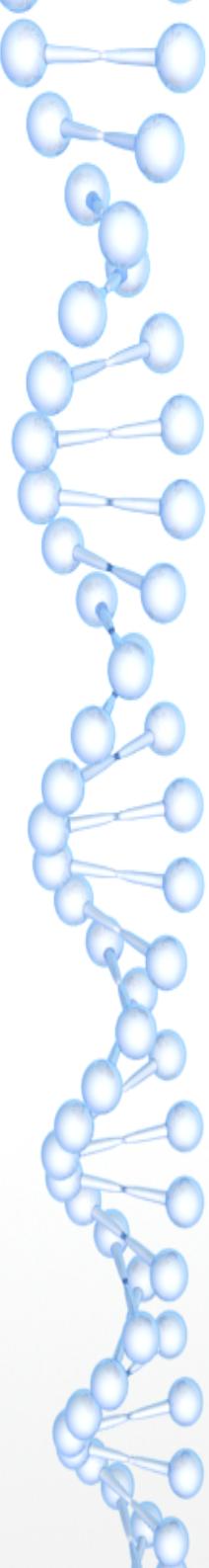


Reuters



SNOWDEN: TRAITOR OR PATRIOT?





Não iremos discutir se ele é ou não.

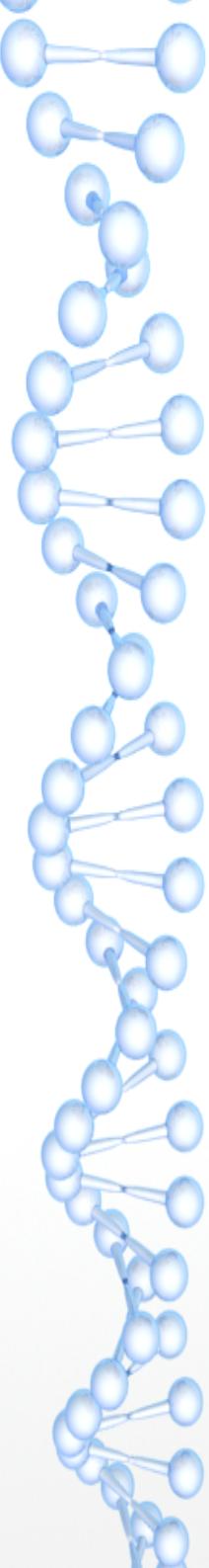
Mas que o mundo da Segurança da informação mudou com sua chegada, mudou...

*** Leis que preveem crimes neste segmento**

- Carolina Dieckmann - **Lei 12.737/2012**
- Marco Civil da Internet - **Lei N° 12.965/14**
- GDPR - Regulamento Geral de Proteção de Dados
(Implementada em 25/05/2018).
- **LGPDP** (Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018).
- **Artigos 11 e 13(17)** "filtro de upload", "taxa de link" e Copyright de qualquer tipo de conteúdo publicado na internet (Vídeos no Youtube, blogs, etc..)

*** Cursos/Treinamentos/Eventos**

- * Entendimento das Normas da família ISO/IEC 27.000 (*)**
- * Elaboração de Políticas de Segurança da Informação (PSI)**
- * Elaboração dos Planos de Continuidade do Negócio (PCN)**



Quem lançou na mídia o Snowden?

Glenn Edward Greenwald



≡ The
Intercept_
Brasil

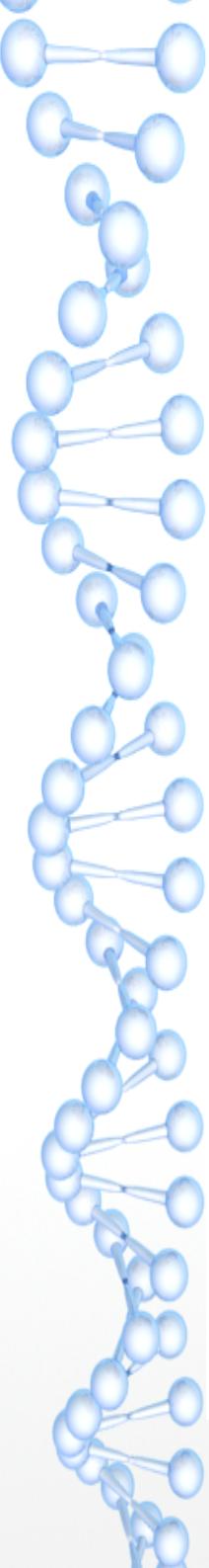
ARTIGOS EM DESTAQUE



**As mensagens secretas
da Lava Jato**
Como e por que o
Intercept está publicando
chats privados sobre a
Lava Jato e Sergio Moro



Junte-se a nós na luta por
transparência e
informação



Hackers (de araraquara)

≡ MENU

CAPA GZH.

GAUCHAZH.
POLÍTICA

ENTRAR

ASSINE

POLÍTICA

Hackers aproveitaram falha de operadoras para ter acesso a dados privados, diz PF

⌚ 24/07/2019 - 14h42min

Publicidade

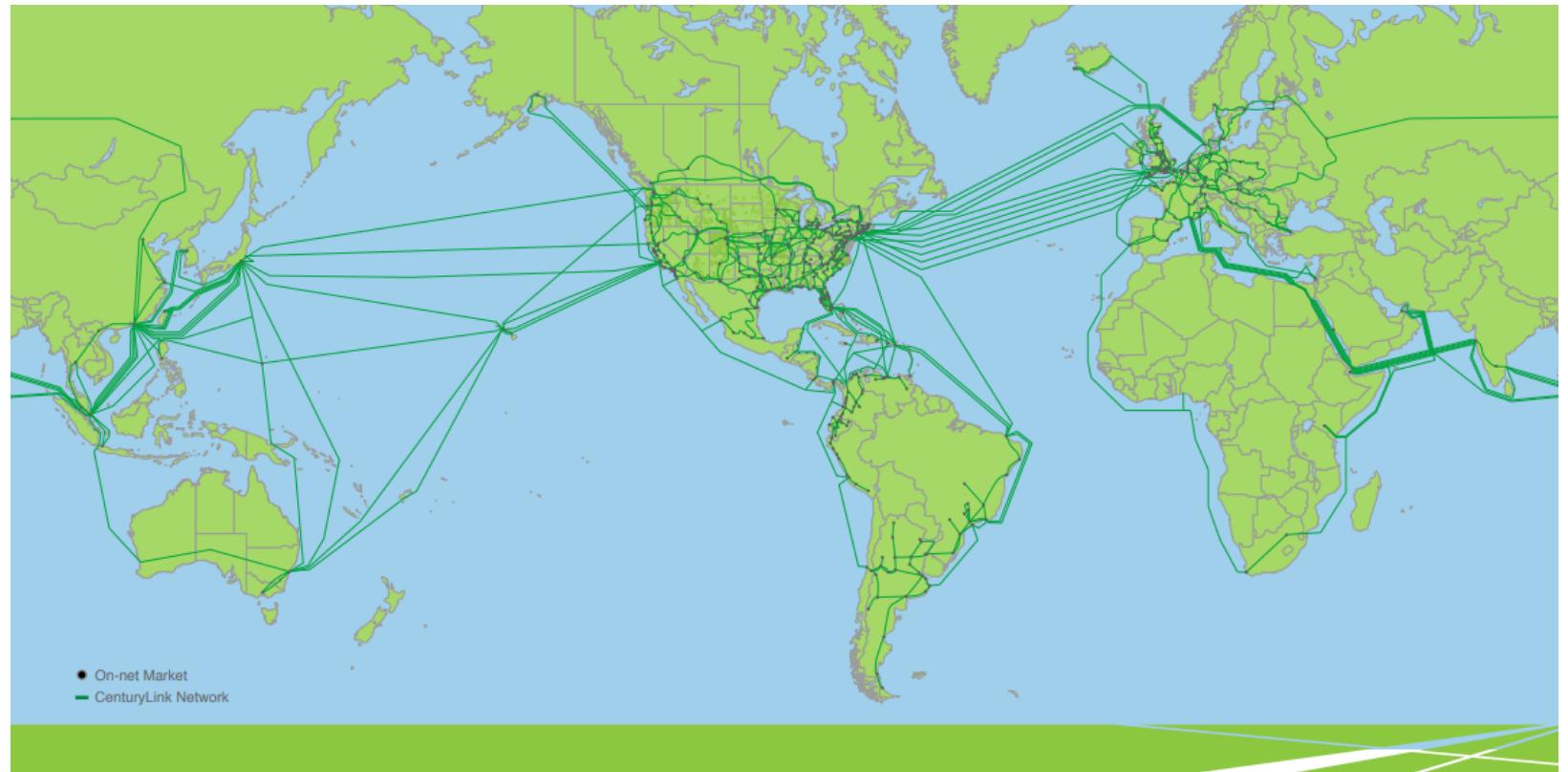
BRASÍLIA, DF (FOLHAPRESS) - Os suspeitos de hackear celulares do ministro da Justiça, Sergio Moro, e de outras autoridades capturaram o código de acesso enviado pelo aplicativo de mensagens Telegram aos seus usuários para sincronização com o serviço Telegram Web - usado no computador. Dessa forma, conseguiram abrir os dados das vítimas nas suas próprias máquinas.

Segundo investigação da Polícia Federal, para aplicar o golpe os invasores se aproveitaram de uma fragilidade comum a todas as operadoras telefônicas.

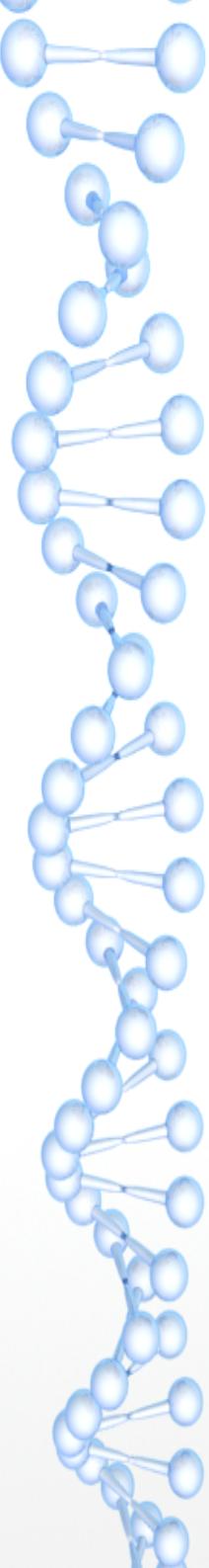
Quando uma pessoa liga para ela própria, não se exige senha para ouvir recados na caixa postal. Foi essa a porta de entrada para se chegar às informações.

Mas estamos no Brasil ...

Não seremos afetados por isso...



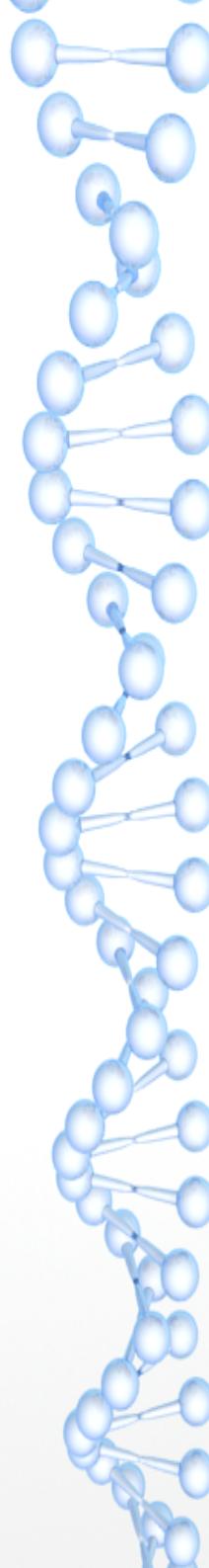
© 2017 CenturyLink. All Rights Reserved. Map information above is current as of October 2017. Information is subject to change. Contact CenturyLink for updates or details. CenturyLink's global network is made up of owned, leased access and iRU segments, which are not distinguished on this map. CenturyLink engages in-region carriers to provide services in some markets.



Qual destes serviços estão operando no BR?

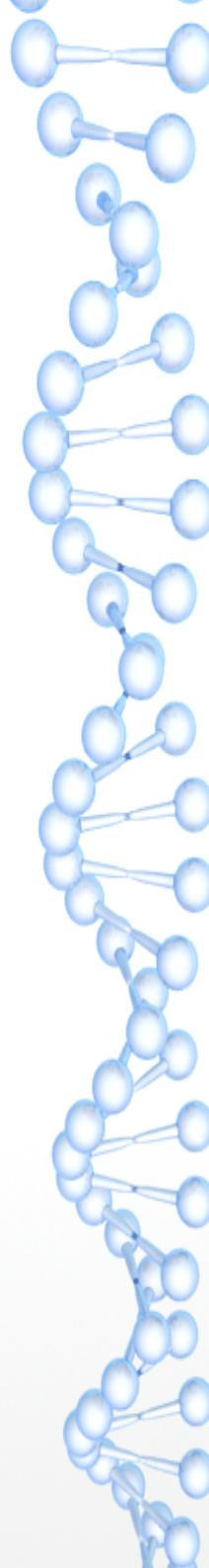
Quem aqui tem conta em uma destas redes?



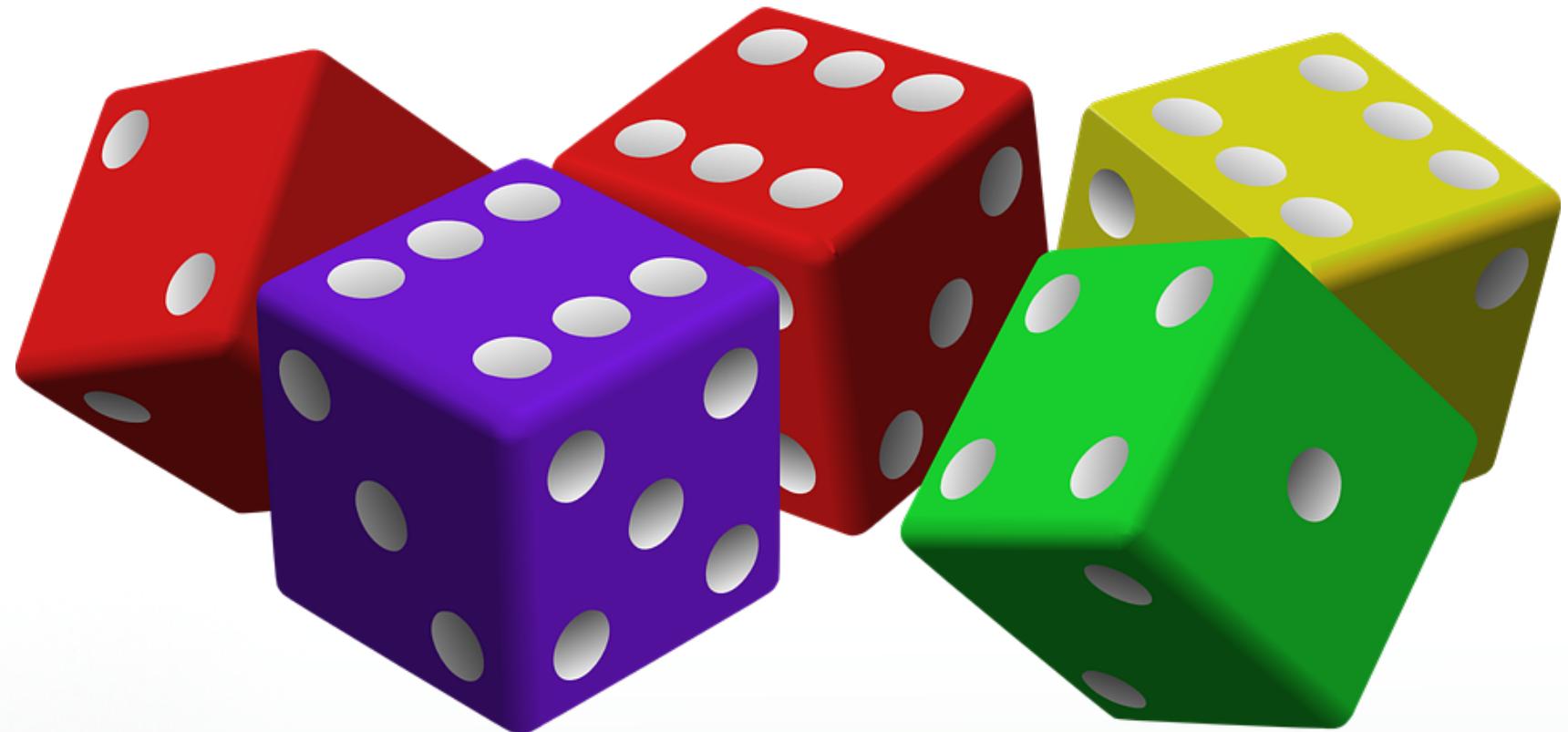


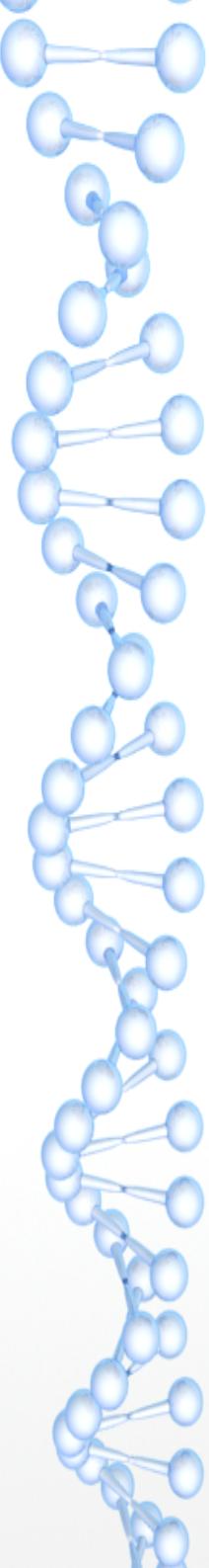
Alguns dos senhores tiveram que pagar \$\$ para ter acesso a rede?





Vocês têm certeza?





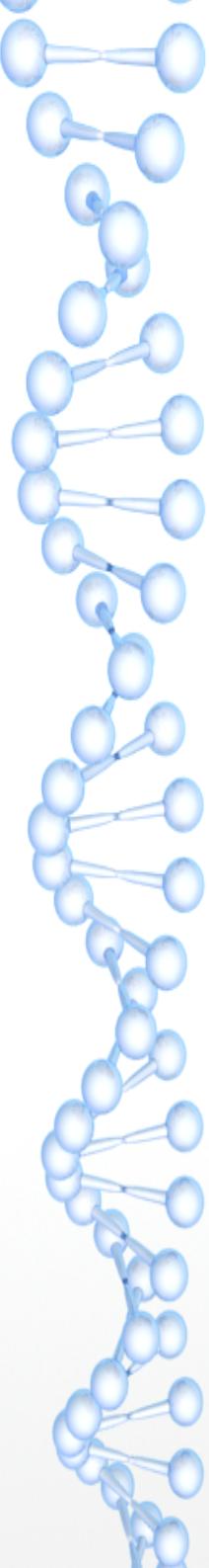
Tudo bem, mas como posso ter mais segurança na Internet?

- * Pesquise sobre a fonte antes de clicar no link ;
- * Troque suas senhas com frequência e use duplo fator de autenticação;
- * Senhas são pessoais e intransferíveis (segredo contado, deixa de ser segredo ... não é mesmo?)
- * Senhas não são compartilháveis ...**

nem com: amigos, familiares, esposas/os, filhos, gatos,cachorros, periquitos....)

- * Se existe uma norma/política SIGA, afinal se ela foi entregue/lida ou solicitada a você, logo tem um objetivo.

Cadeado Verde = Seguro?



A screenshot of a web browser window showing the URL https://www.google.com.br/gws_rd=ssl. The page displays a green lock icon and the text "Conexão segura". Below this, two sections are visible: "Proteção contra rastreamento:" (disabled) and "Permissões" (unchecked). A button at the bottom says "Limpar os cookies e dados do site...". To the right of the browser is a "Visualizador de certificado" (Certificate Viewer) window for the domain *.google.com. The "Detalhes" tab is selected, showing the following details:

Este certificado foi verificado para estes usos:	
Certificado para servidor SSL	
Emitido para	
Nome Comum (CN)	*.google.com
Empresa (O)	Google LLC
Unidade Organizacional (OU)	<Não faz parte do certificado>
Número de série	25:65:A8:5C:DA:B8:81:A5
Emitido por	
Nome Comum (CN)	Google Internet Authority G3
Empresa (O)	Google Trust Services
Unidade Organizacional (OU)	<Não faz parte do certificado>
Período de validade	
Inicio	28 de agosto de 2018
Fim	20 de novembro de 2018
Assinaturas	
Assinatura SHA-256	70:8C:FA:34:2B:01:25:57:D8:C3:A5:F4:0F:35:C7:CC: 18:60:F3:76:97:64:7A:A0:05:AC:43:9C:5A:07:F1:7B
Assinatura SHA1	36:62:15:80:90:FB:C9:3C:32:55:D6:42:34:70:C9:8E:FF:19:90:F5

Senhas são difíceis de decorar

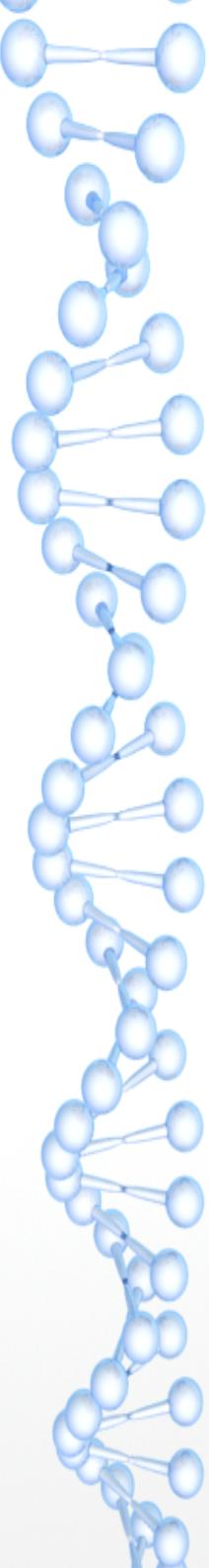
“Prefiro 12345 ou senha como senha...”

“Na minha empresa tem um TXT...”



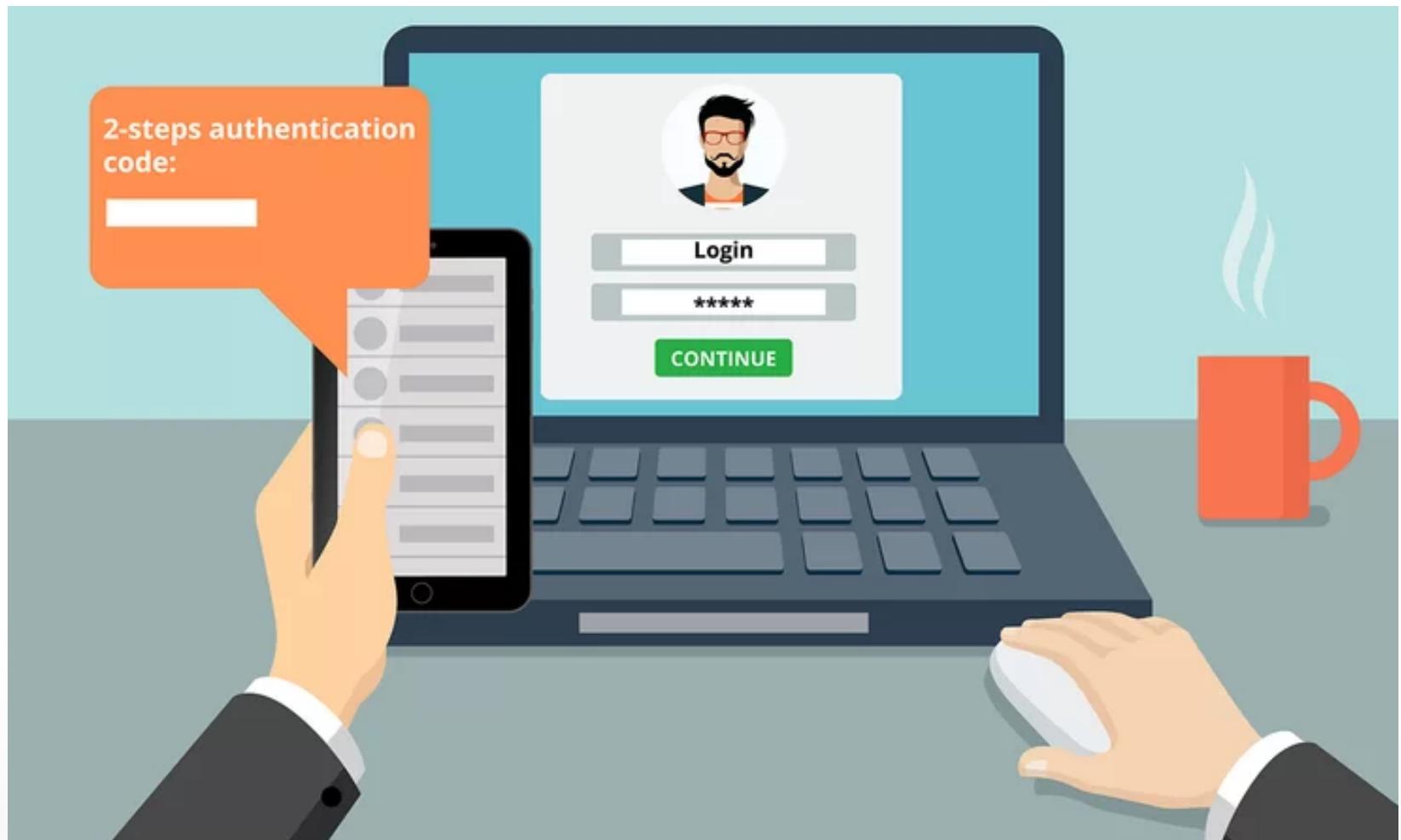
“Salvo tudo lá e depois mando por...”

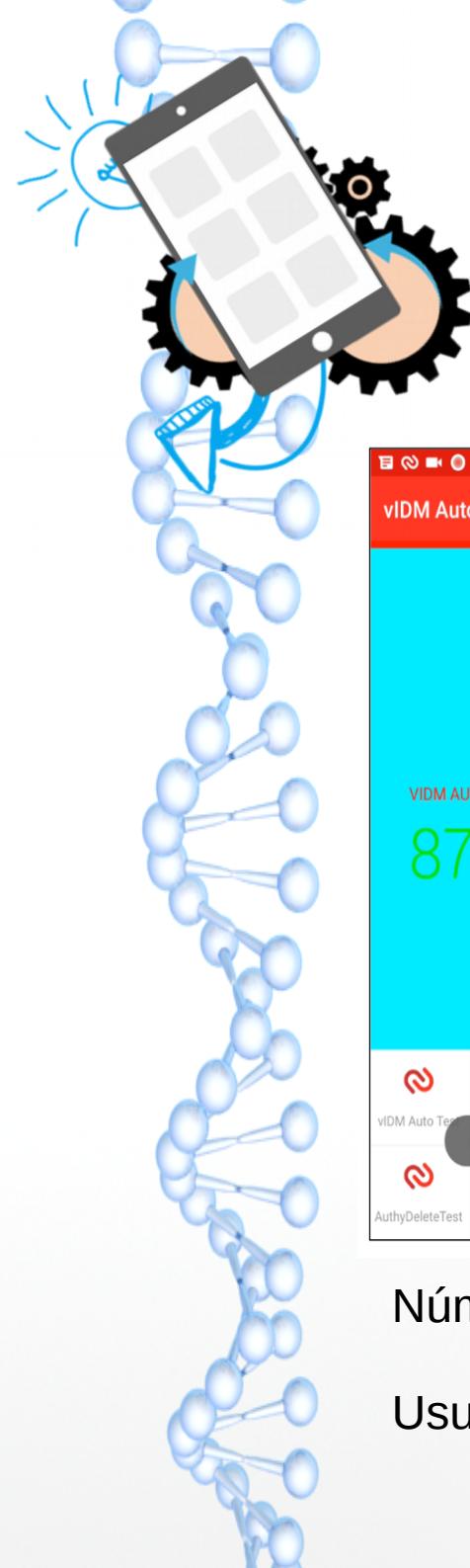




Use duplo fator!

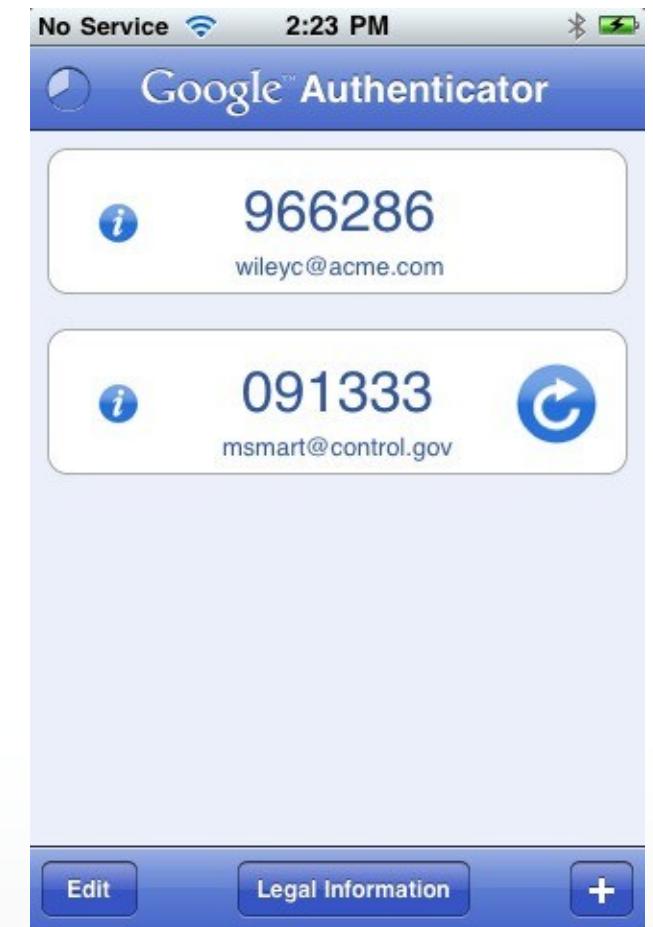
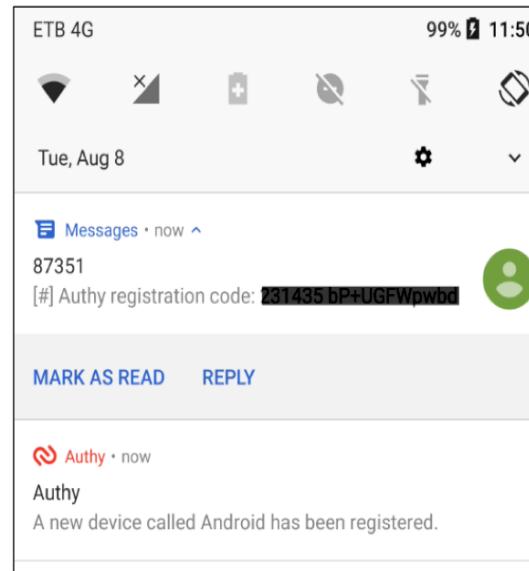
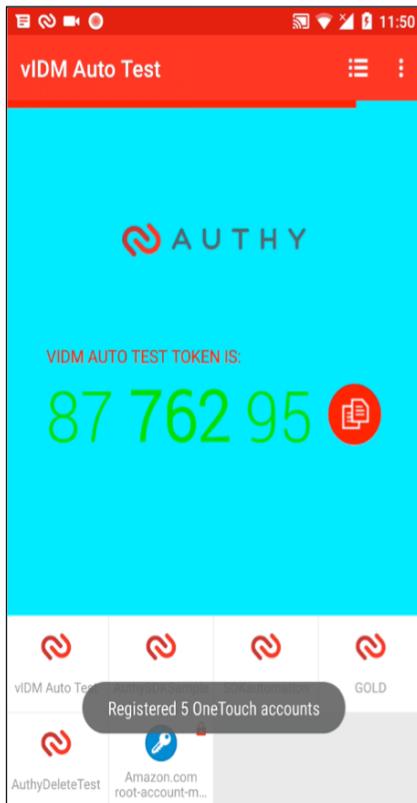
O que é isso?





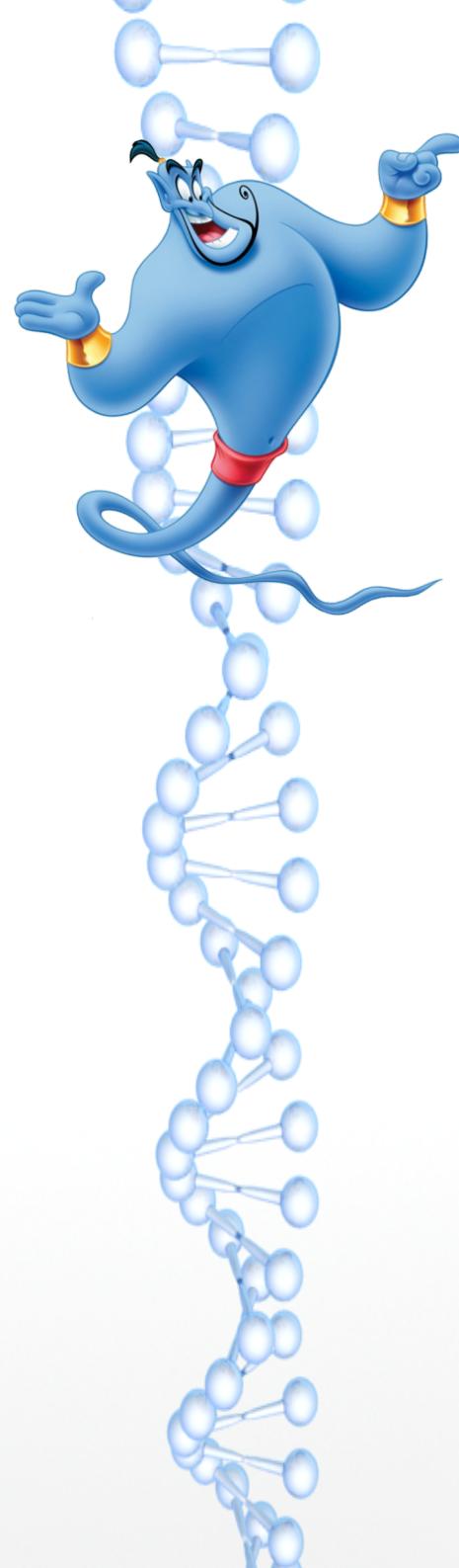
Softwares/App

Authy e Google Auth



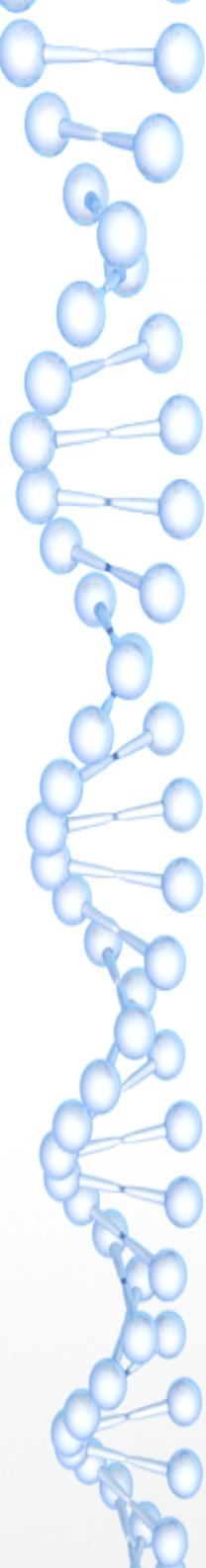
Número Randômico – Altera a cada X tempo

Usuário @ Serviço/Site/Sistema

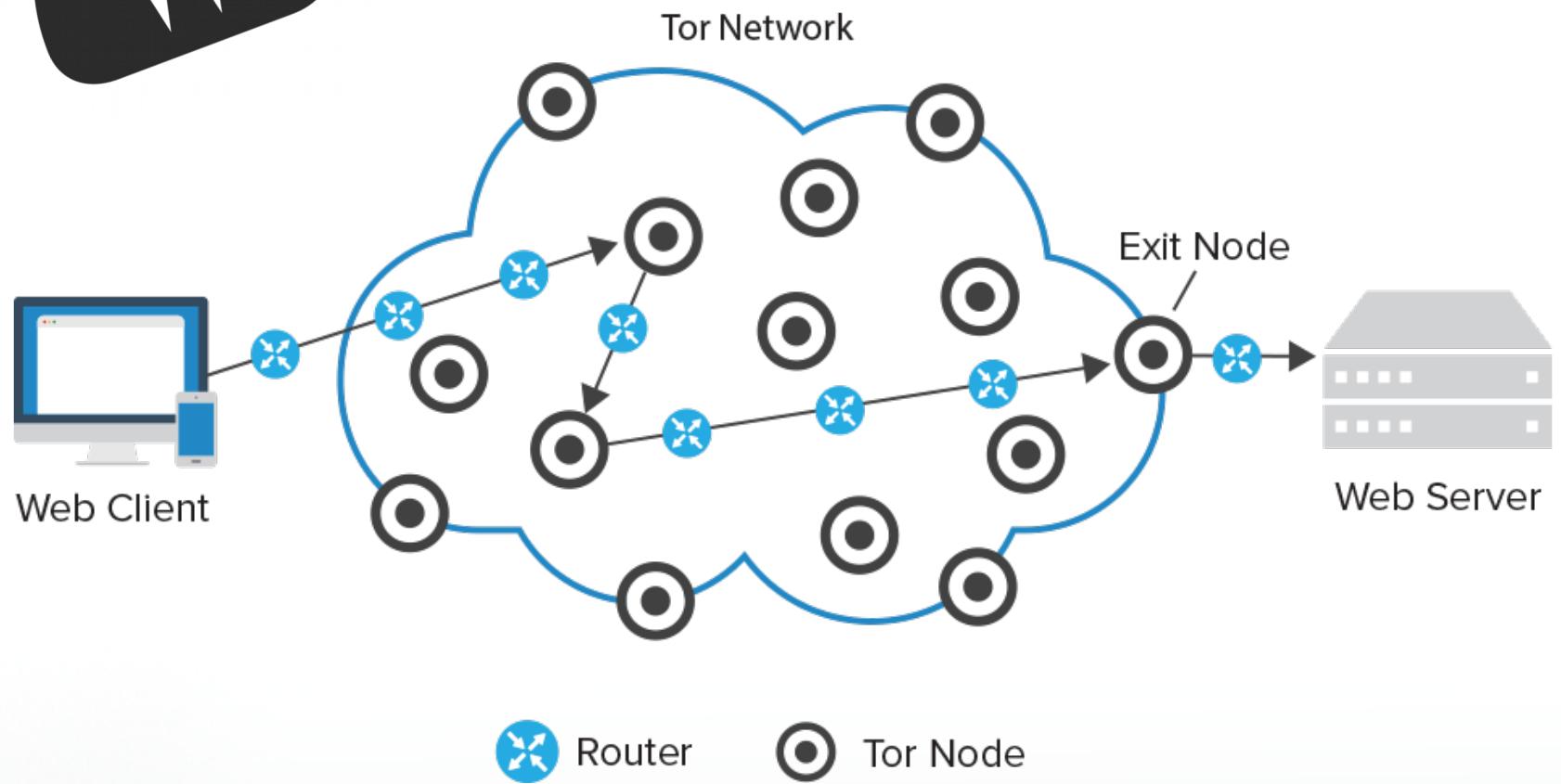
A cartoon illustration of a blue DNA molecule with a face, arms, and legs. It has a wide, smiling mouth and is pointing its right hand towards the text. It wears a red belt and gold bracelets on both wrists.

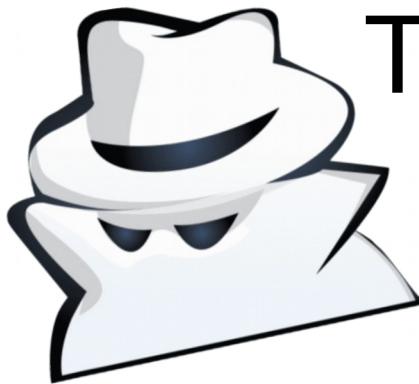
Então tudo é resolvido com a senha?

- * Não;
- * Uma **senha segura** já é um indício de preocupação com a segurança da informação;
- * O principal **vetor de ataque** Hacker/Cracker começa com conhecimento do alvo, entre as atividades destaca-se quais os serviços que o mesmo está cadastrado e se o mesmo possui senhas fracas.



Anoni_mato ou não?



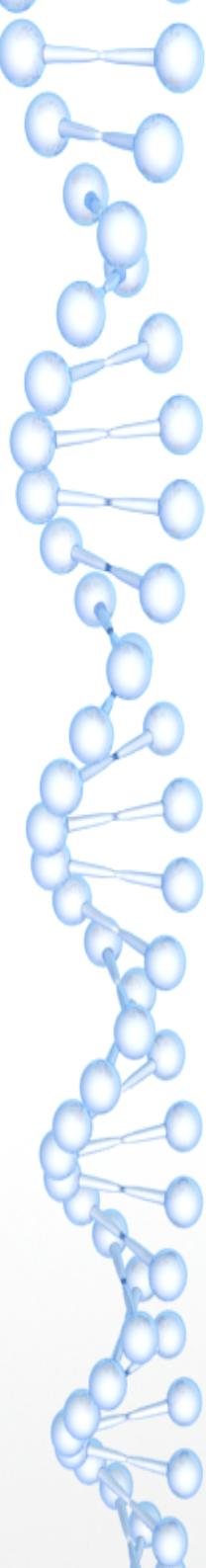


Tor/Onion/Whonix...

Não há como garantir 100% de anonimato;

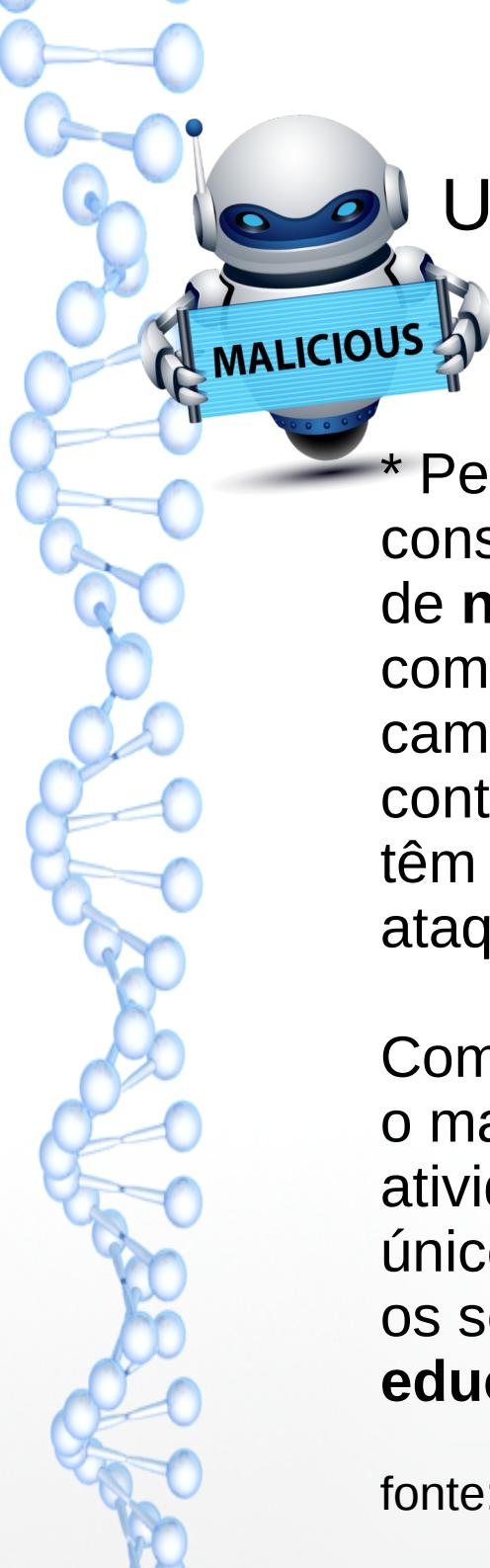
Projeto Tor / Whonix.

O Whonix até mesmo chega a criar múltiplas máquinas virtuais para despistar as atividades dos usuários. E nem mesmo ele é totalmente confiável.



Tipos de ataques na internet

- * **Vírus** (menos relevante atualmente) ;
- * **Golpes** (Cartões de créditos, dados, etc..);
- * **Fishing** (páginas ou e-mails simulando sites oficiais);
- * **Malware** (Código criado para diversos fins, o mais comum é fazer de seu dispositivo um zumbi);
- * **Ransomware** (Sequestro de dados, sistemas, etc..);
- * **Whatsapp** (wishing);
- * **Vulnerabilidades** em sistemas e/ou hardwares;
- * **BOTS – IA.**

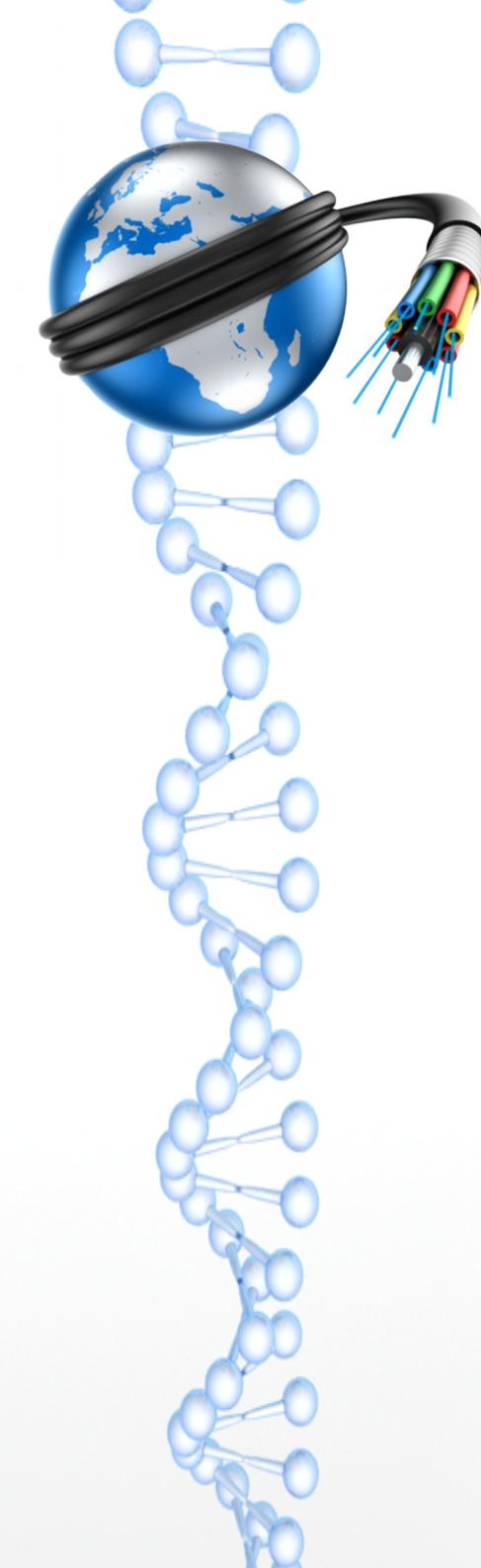


Bots & IA

Uma solução tecnológica que se tornou um problema de SegInfo.

* Pesquisadores dizem, que 20,4% do tráfego online é constituído por **bots maliciosos**, voltados para ataques de **negação de serviço, roubo de dados** e compartilhamento de **fake news**. Ataques virtuais e campanhas de disseminação de **phishing** também contam fortemente com tais tecnologias, que, logicamente, têm seus setores de preferência para a realização de ataques e operações.

Como não poderia deixar de ser, o segmento **financeiro** é o mais atingido por golpes desse tipo, com 42,2% de atividade dos bots maliciosos. Entretanto, ele não é o único e os números são bem aproximados também para os setores de **ingressos e bilhetagem** (39,3%), **educação** (37,9%), **TI** (34,4%) e **marketing** (33,3%).



Alguns ataques na internet

G1

ECONOMIA

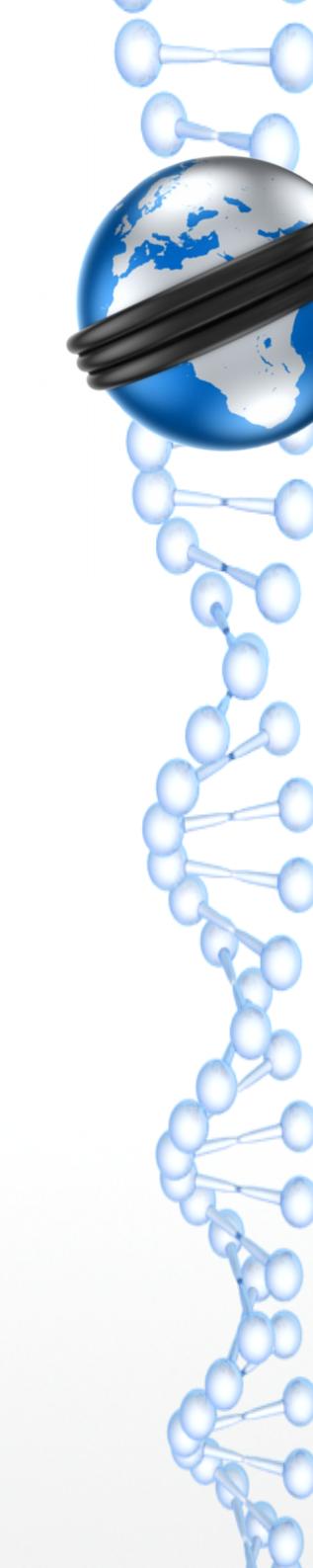
BLOG DO ALTIERES ROHR

Como os golpistas ganham dinheiro com as fraudes no WhatsApp?

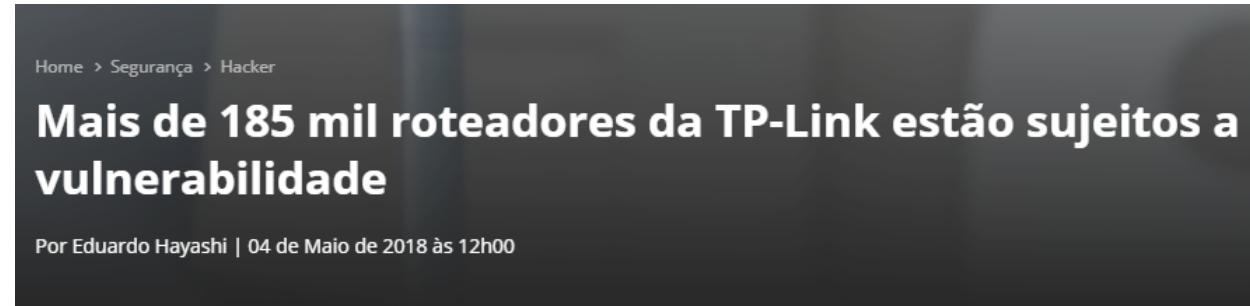
09/06/2018 08h00 · Atualizado há 4 meses



Criminosos se aproveitam de acordos de publicidade para faturar com golpes no WhatsApp — Foto: Altieres Rohr/Especial para o G1



Alguns ataques na internet



Home > Segurança > Hacker

Mais de 185 mil roteadores da TP-Link estão sujeitos a vulnerabilidade

Por Eduardo Hayashi | 04 de Maio de 2018 às 12h00

TUDO SOBRE



TP-Link

ATUALIZAÇÃO (04/05): A TP-Link entrou em contato com a redação do Canaltech e informou que sua equipe de engenheiros e pesquisadores já está desenvolvendo uma correção para a vulnerabilidade presente no roteador TL-WR740N. Ainda de acordo com a empresa, a atualização de firmware deve ser disponibilizada ainda neste mês de maio. Enquanto o update não chega, a companhia solicita que os clientes façam a alteração do usuário e senha padrão do equipamento para impedir o acesso de pessoas não autorizadas.

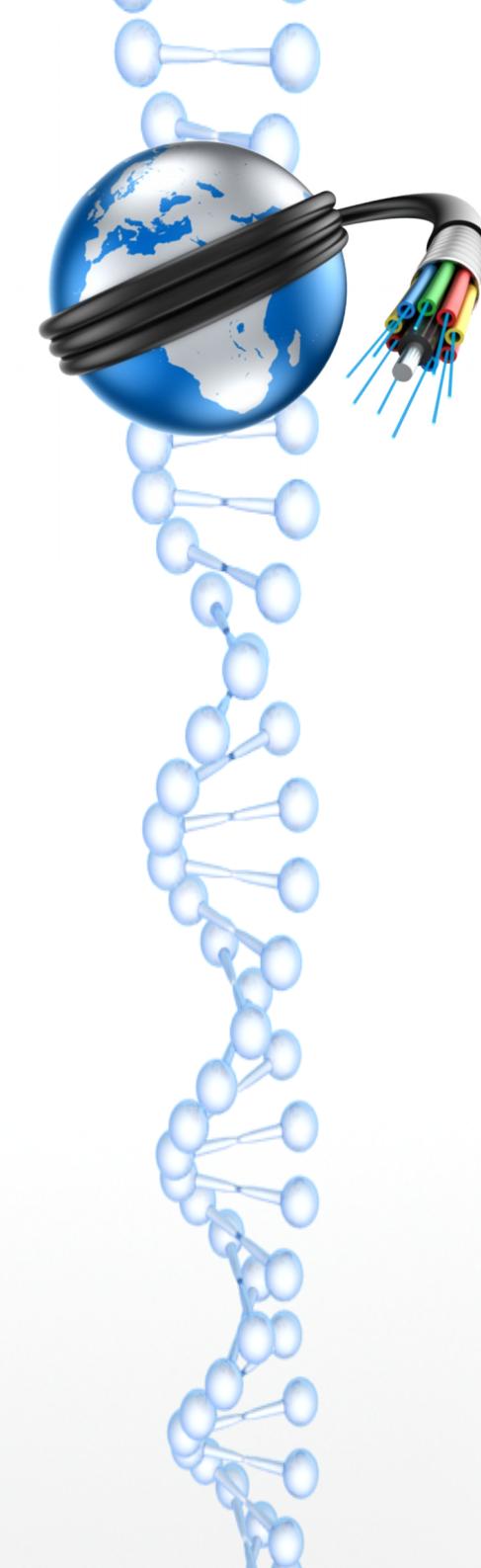
Nota original

Uma vulnerabilidade crítica de segurança foi identificada em roteadores TP-Link, afetando mais de 185 mil aparelhos da empresa.

Participe do nosso [GRUPO CANALTECH DE DESCONTOS](#) do [Whatsapp](#) e do [Facebook](#) e garanta sempre o menor preço em suas compras de produtos de tecnologia.

De acordo com a publicação do pesquisador de segurança digital Tim Carrington, os roteadores da série TL-WR740N possuem uma brecha que viabiliza a execução remota de códigos, sendo esta uma óbvia porta de entrada para possíveis invasões.

Durante a análise do código-fonte do TL-WR740N, o especialista descobriu que a falha é muito semelhante à que foi encontrada no modelo TL-WR940N, uma vez que ambos os equipamentos de rede compartilham de códigos semelhantes.



Alguns ataques na internet

techtudo

DOWNLOADS

TP-Link libera lista de roteador afetados por falha no Wi-Fi com WPA2

Fabricante prepara atualizações de firmware para os produtos e faz recomendações de segurança.

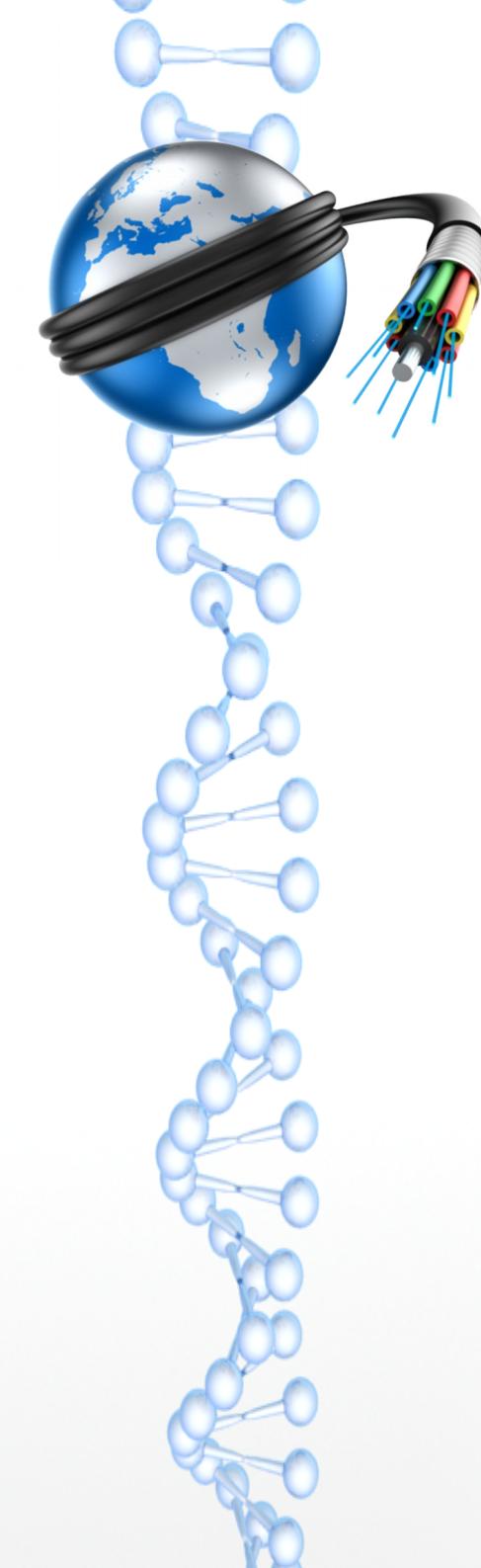
Por Filipe Garrett, para o TechTudo

19/10/2017 14h19 · Atualizado há 11 meses



A **TP-Link** emitiu uma nota oficial reconhecendo que parte de seus produtos é afetada pela vulnerabilidade KRACKs, que permite a invasores a **capacidade de interceptar informações em redes Wi-Fi**. Além disso, a marca identificou os modelos de roteadores e outros equipamentos de rede sem fio que podem ser alvo bem-sucedidos de ataques em WPA2, salientando que todos esses aparelhos receberão atualizações de firmware para eliminação do problema dentro das próximas semanas.





Alguns ataques na internet

techtudo

INFORMÁTICA

Criminosos usaram falha em roteadores D-Link para roubar dados bancários

Falha ocorreu entre 8 de junho e 10 de agosto; a recomendação é atualizar o firmware e trocar a senha

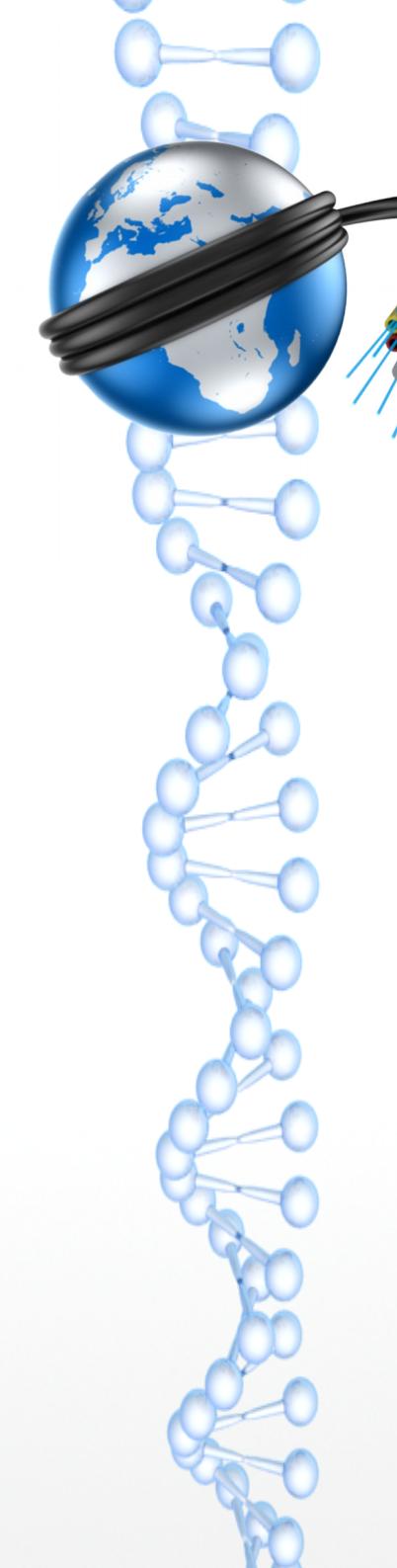
Por Igor Nishikiori, para o TechTudo

14/08/2018 14h51 · Atualizado há 1 mês



Cibercriminosos exploraram uma falha nos roteadores da marca **D-Link** para possivelmente roubar dados de clientes de bancos brasileiros, afirmou a empresa de segurança digital Radware. Segundo a empresa de proteção na web **ESET**, a vulnerabilidade permitiu aos golpistas manipularem o servidor DNS dos dispositivos conectados aos roteadores, redirecionando o usuário a páginas falsas do **Banco do Brasil** e do **Itaú**, prática conhecida como **hijacking** (sequestro, em inglês).

Anúncio fechado por Google



Alguns ataques na internet

tecnoblog

TECNOCAST REVIEWS CUPONS CURSOS ASSISTENTE DE COMPRAS ANUNCIE



280 mil roteadores foram invadidos para minerar criptomoeda, a maioria no Brasil

Roteadores da MikroTik foram infectados com minerador de criptomoeda; falha foi corrigida em abril mas ainda é usada



Por Felipe Ventura
11/09/2018 às 17h24

NEWS

Já conhece a nova extensão do **Tecnoblog**?

Baixe Agora

Mais de 280 mil roteadores da MikroTik estão infectados com um minerador de **criptomoeda**. A mesma falha de segurança está sendo usada em diferentes ataques, que atingem principalmente o Brasil. Ela já foi corrigida em abril, mas muita gente não instalou a atualização.

- Roteadores da MikroTik estão desviando tráfego; Brasil é um dos mais afetados

O pesquisador Troy Mursch catalogou [64 versões diferentes](#) dessa invasão, que usa o navegador web para minerar criptomoeda. A mais recente das elas afeta quase 6.500 dispositivos, 4.500 deles no Brasil.



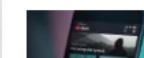
DOMAIN.COM

SAVE 25%
on domains, websites,
email, & more

Use Code: GETSTARTED

GET STARTED

Em Destaque



YouTube Music Premium e
YouTube Premium
removem...



iPhone XS, XS Max, XR, Watch
Series 4: o resumo dos...



Novo padrão de placas de
carro começa a ser usado
no...



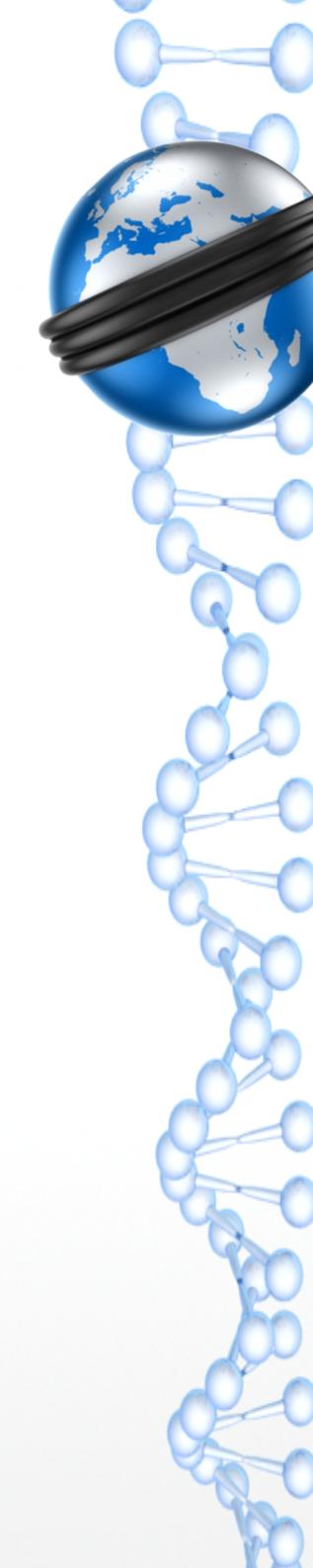
TV Sony X905F: escolha pela
imagem



Dez anos de Google Chrome:
como o navegador dominou
o...



O que é a falha Foreshadow
que afeta processadores...



Alguns ataques na internet

≡ MENU |||

TECNOLOGIA E GAMES

29/01/2013 14h25 - Atualizado em 05/02/2013 19h26

Brecha vaza na web imagens gravadas por sistemas de segurança

Problema pode afetar 18 fabricantes de gravadores digitais (DVRs). Segundo especialista, 58 mil sistemas estariam expostos.

Altieres Rohr
Especial para o G1

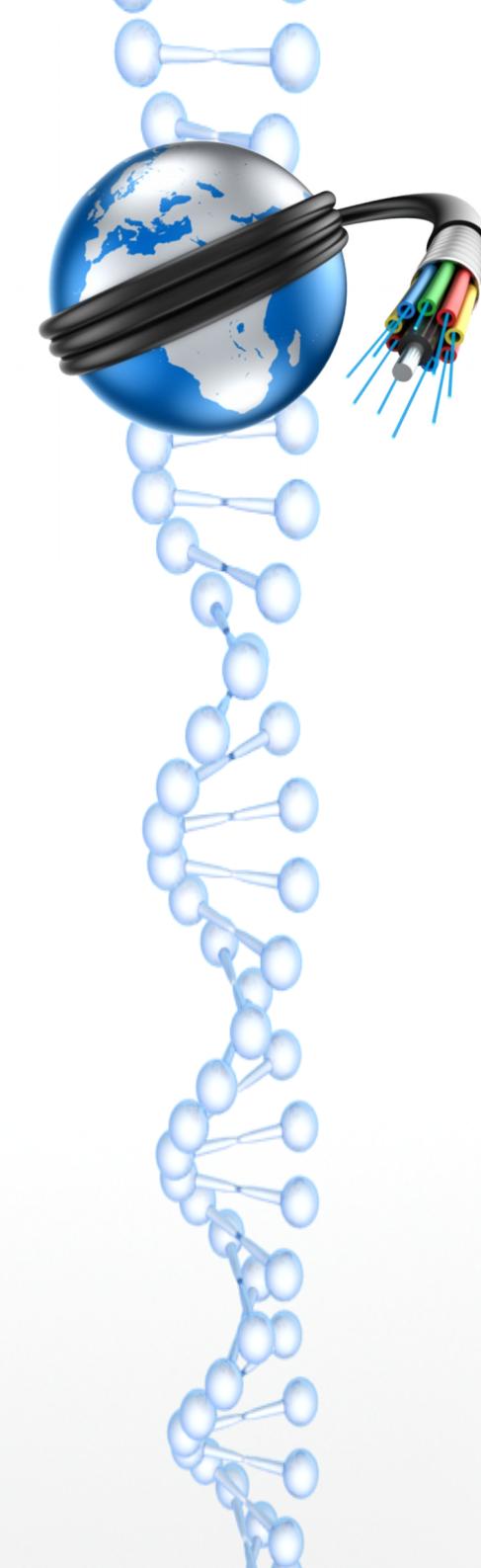


Sistemas de gravação digital, usados para a segurança de estabelecimentos, por exemplo, podem ser hackeados (Foto: Divulgação)

Um pesquisador de segurança que usa o apelido de "someLuser" descobriu uma vulnerabilidade em sistemas de gravação digital (DVR, na sigla em inglês) comumente usados em conjunto com câmeras de segurança em circuitos fechados de televisão (CFTV). A falha permite descobrir a senha do aparelho, o que dá acesso total às imagens gravadas, permitindo inclusive alterá-las ou removê-las da memória do dispositivo.

A vulnerabilidade está presente em um software fornecido por uma empresa chinesa chamada Ray Sharp. Segundo o especialista em segurança H. D. Moore, 18 fabricantes diferentes fazem uso do sistema chinês.

Os fabricantes, porém, ainda não confirmaram a falha.



Alguns ataques na internet

Smart-TVs em alto risco de invasão

11/01/2016 Autor: David B.Svaiter - Sócio-Diretor da área de S.I. & Criptografia da Big Blue

As Smart-TV's rodando o sistema operacional Android fornecem funcionalidades adicionais aos usuários, além de TVs normais, mas também criam um risco de segurança, conforme a Trend Micro revela.

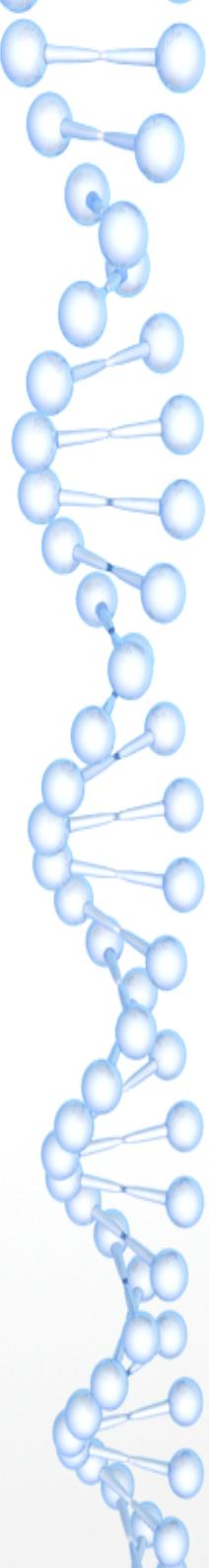
A Internet das Coisas (IoT) está em rápido crescimento e as TVs Inteligentes representam uma peça central neste crescimento, até porque elas são mais do que dispositivos de visualização passiva, já que podem executar aplicativos Android.

Um post no blog de autoria de Ju Zhu (da TredMicro) explica que alguns dos aplicativos mais populares no Smart TVs permitem aos usuários assistir a canais de outras partes do mundo, mas também quebrar a segurança. De acordo com o pesquisador de segurança, alguns desses aplicativos contêm uma *backdoor* que abusa de uma falha em versões mais antigas do Android. A vulnerabilidade ([CVE-2014-7911](#)) é encontrado no Android anterior da versão Lollipop 5.0 (variando de 1.5 a Cupcake KitKat 4.4.2) e permite a um invasor executar código arbitrário em dispositivos comprometidos.



O problema é que muitas das *Smart TV's* de hoje executam versões mais antigas do Android, o que significa que elas são afetados pela falha de segurança. A Trend Micro descobriu TVs vulneráveis de marcas como Changhong, Konka, Mi, Philips, Panasonic e Sharp, mas diz que outros dispositivos que executam versões mais antigas do Android também estão em risco, mesmo se esses aplicativos são usados principalmente em TVs.





Você convidaria um sequestrador,
para morar junto com você na
sua casa?

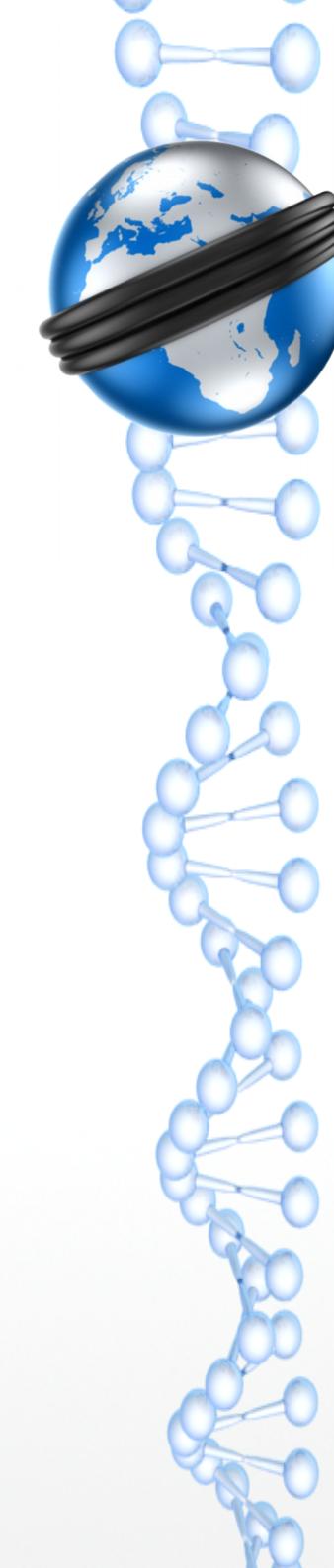


Então porque ainda tem um “aparelhinho” (Tv-Box, Setup-Box) que pega todos os canais?



Informações extras:

<https://www.cianet.com.br/blog/operacao-de-tv/entenda-criptografia-iptv-cas> ⁵⁰



Alguns ataques na internet

TV BOX PIRATAS ATACADOS POR VIRUS PARA MINERAR CRIPTOMOEDAS

Por **Richard Lima** - fevereiro 28, 2018

2750

f Compartilhar no Facebook

t Tweet

G+

P

Curtir 25

Tweet



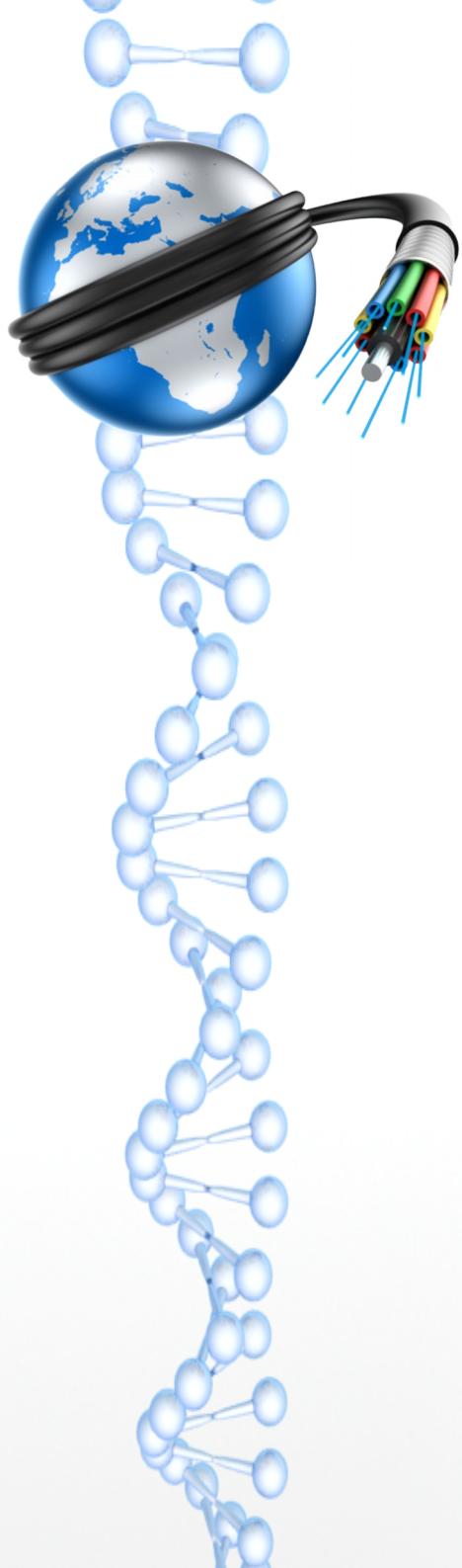
Hoje a internet estava cheia de matérias sobre Smart TVs atacadas por vírus para minerar criptomoedas para hackers, fui dar um conferida nas matérias e vi que a vulnerabilidade estava nas Smart TVs com firmware feito com o sistema operacional Android TV, aí pensei, opa, peraí, sistema operacional Android... Android TV... Android TV Box... TV Box para tv pirata, será??? Vou verificar.

Pois é... é.

O negócio tá mesmo complexo quando se fala em conectar qualquer aparelho à internet por que a galera que entende de invadir sistemas pouco seguros para instalar programas que escravizam estes aparelhos para trabalhar para eles está cada dia mais esperta e mais ousada.

As Smart TVs tem um sistema teoricamente um pouco mais seguro pois recebem versões certificadas do Android TV onde são feitas poucas modificações para implementar o layout e aplicativos da marca que vai usar o Android TV em suas televisões, agora quando se trata dos TV Box que usam versões do Android sem certificação... Aí o negócio complica.

Quando se fala nessa nova onda de virus para minerar criptomoedas nenhum dispositivo conectado à internet está à salvo, mas o caso das TV Box merecem especial atenção.



Carrefour anuncia dispositivo no melhor estilo 'gatonet', capaz de piratear sinal de TV a cabo

Vendedor chega até mesmo a anunciar o dispositivo na central de som do estabelecimento. Set up box seria capaz de desbloquear até '8 mil canais'

Alguns ataques na internet

Vulnerabilidade no Uconnect permite hackers controlarem carros da Fiat, Jeep e Chrysler

21/07/2015 13:43 | João Gabriel | @joao_gan | Reportar erro

◀ POST ANTERIOR

Alcatel Onetouch lança o IDOL 3 no Brasil

Trilha sonora de The Last of Us será lançada amanhã em dis



0

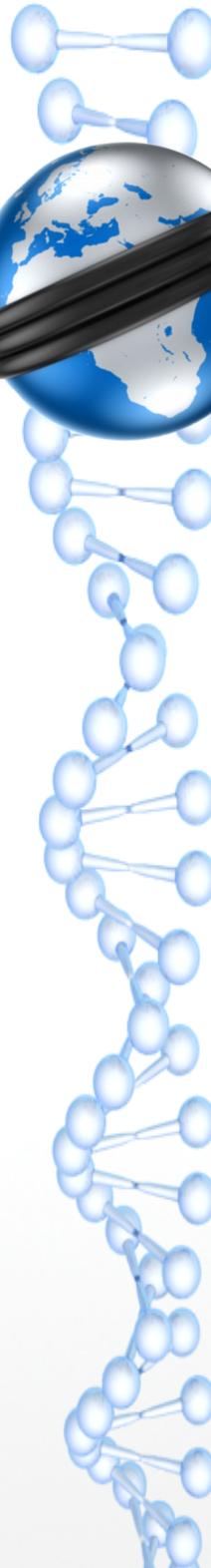
Like

Share

Tweetar

G+

Dois hackers anunciaram que vão divulgar nas próximas semanas uma vulnerabilidade que encontraram no sistema conectado da Fiat Chrysler, o Uconnect, que aparece em veículos levando a marca Jeep, Dodge e Ram também. São aproximadamente 471.000 carros afetados que podem ser remotamente controlados pelos invasores, inclusive em partes críticas, como os freios, o volante e a transmissão.



Alguns ataques na internet

G1

DISTRITO FEDERAL

Netshoes ligará para 2 milhões de clientes afetados por vazamento de dados

Ligações serão feitas a partir de 8 de março. Medida foi adotada após reunião da empresa com Ministério Público do DF.

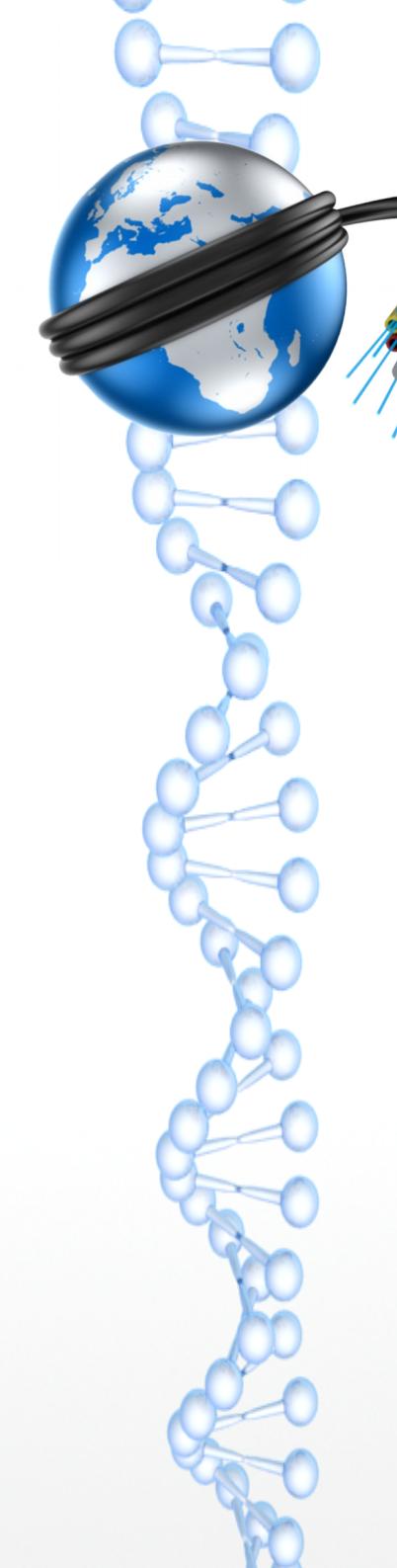
Por G1 DF e TV Globo

28/02/2018 05h25 · Atualizado há 7 meses



Hackers conseguiram dados de quase 2 milhões de contas no site — Foto: Reprodução/Fantástico

O site de comércio eletrônico Netshoes informou, por meio de nota, que os quase 2 milhões de consumidores de todo o país atingidos pelo **vazamento de dados** serão contatados por telefone a partir de 8 de março. Depois dessa data, a empresa terá mais 30 dias úteis para finalizar as ligações.



Alguns ataques na internet



The screenshot shows the Tecnoblog homepage with a search bar and social media links at the top. Below is a promotional banner for Domain.com offering a 25% discount with code SEARCH, featuring a man in glasses looking at a computer screen. The main news headline is "Facebook obriga 90 milhões de usuários a fazer login de novo após invasão".

Início » Segurança » Facebook obriga 90 milhões de usuários a fazer login de novo após invasão

Facebook obriga 90 milhões de usuários a fazer login de novo após invasão

Facebook diz que foi hackeado através do recurso "Ver como", agora desativado, e não confirma vazamento de dados



Por Felipe Ventura
28/09/2018 às 14h01

NEWS

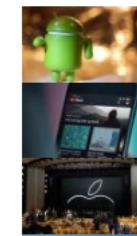
Já conhece a nova extensão do Tecnoblog? [Baixe Agora](#) 

O Facebook sofreu um ataque em sua rede de computadores que afetou 50 milhões de pessoas. A rede social deslogou 90 milhões de usuários, forçando-os a fazer login de novo, mas ainda não sabe se houve vazamento de dados. Os hackers usaram uma falha que permitia assumir controle do perfil dos outros.

- [Como recuperar a senha do Facebook](#)
- [Como recuperar uma conta do Facebook sem o e-mail de cadastro](#)



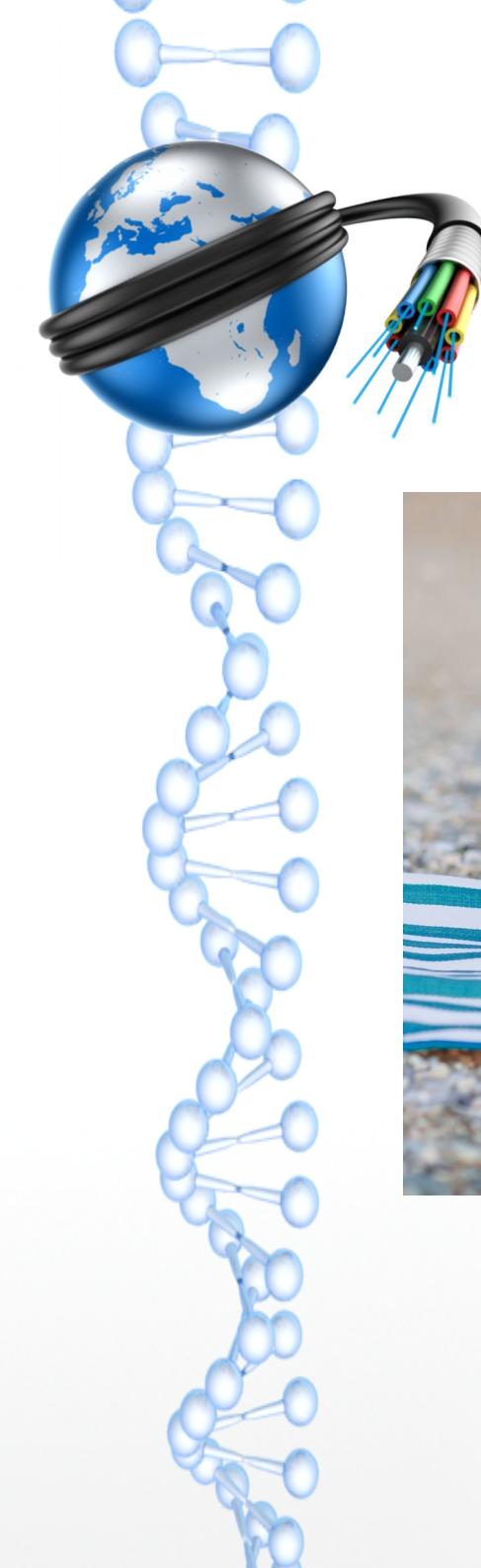
Em Destaque



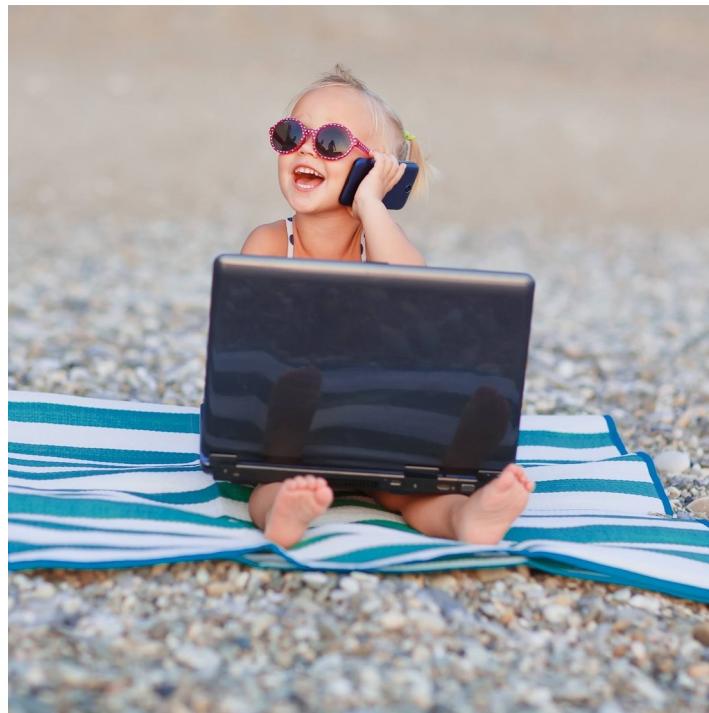
Dez anos de Android: como surgiu o sistema móvel mais...

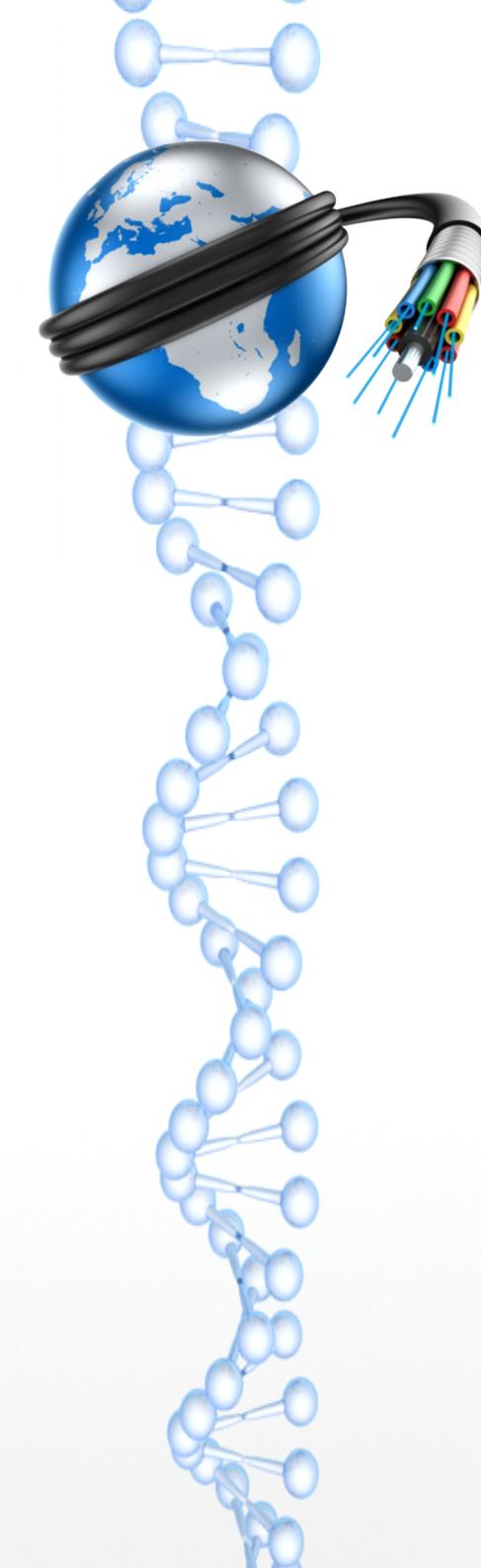
YouTube Music Premium e YouTube Premium removem...

iPhone XS, XS Max, XR, Watch Series 4: o resumo dos...



To na safe meu amigo!





Caso RGNV-Transportes

Nota de Esclarecimento
02 de abril de 2019

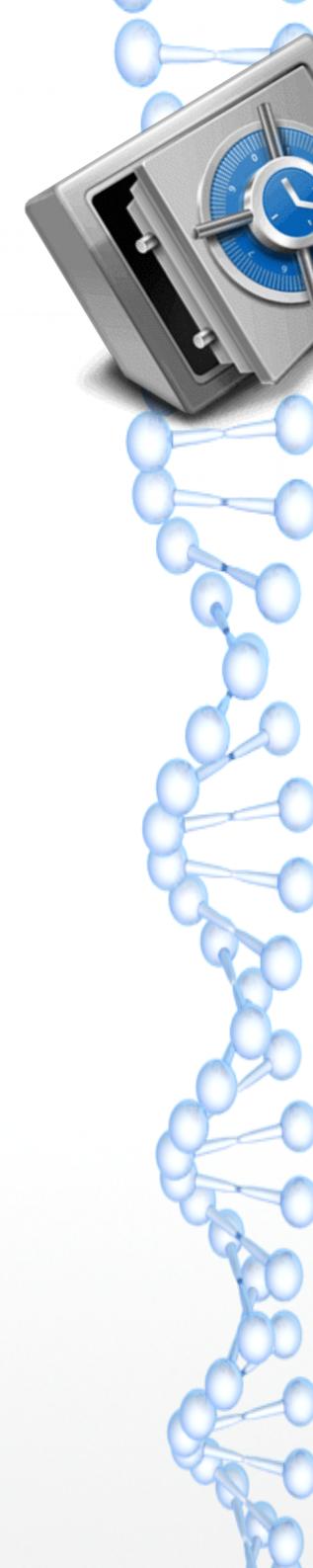
Os serviços de venda de créditos eletrônicos e carregamento de cartões dos usuários do transporte coletivo prestam-se com enormes limitações desde o dia 20.03.2019. A empresa foi vítima de crime cibernético, inclusive com exigência

de resgate para a liberação do sistema. As medidas cabíveis foram tomadas de imediato, porém como se trata de milhões de informações, o restabelecimento do sistema é lento e, às vezes, impossível de execução sem antes realizar a substituição de equipamentos. Apesar disso, os cartões do passe escolar

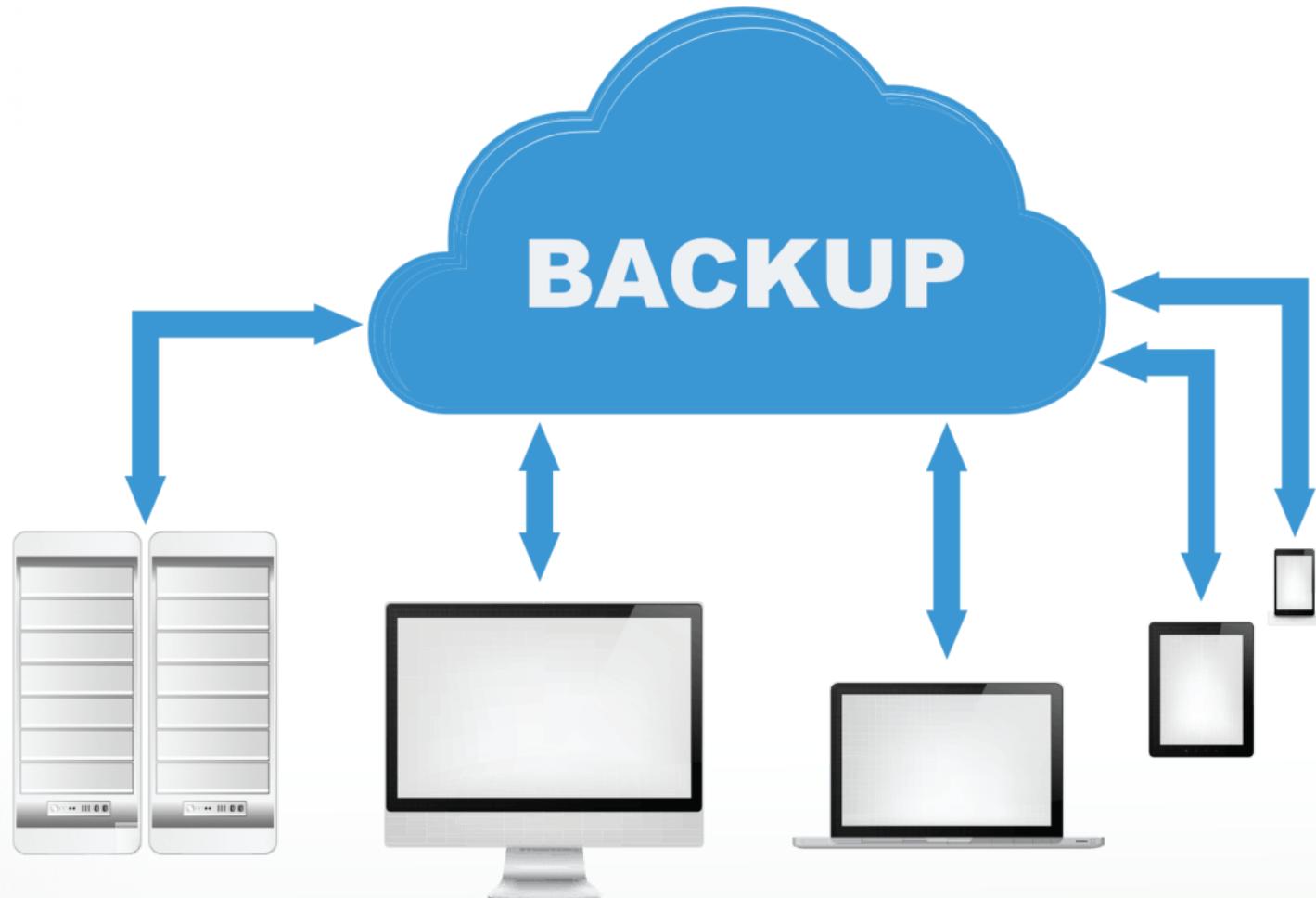
tiveram somente duas interrupções totais no período, uma de 24 horas contínuas e outra de oito horas seguidas. Os cartões com créditos do vale-transporte também foram carregados no período em alguns momentos.

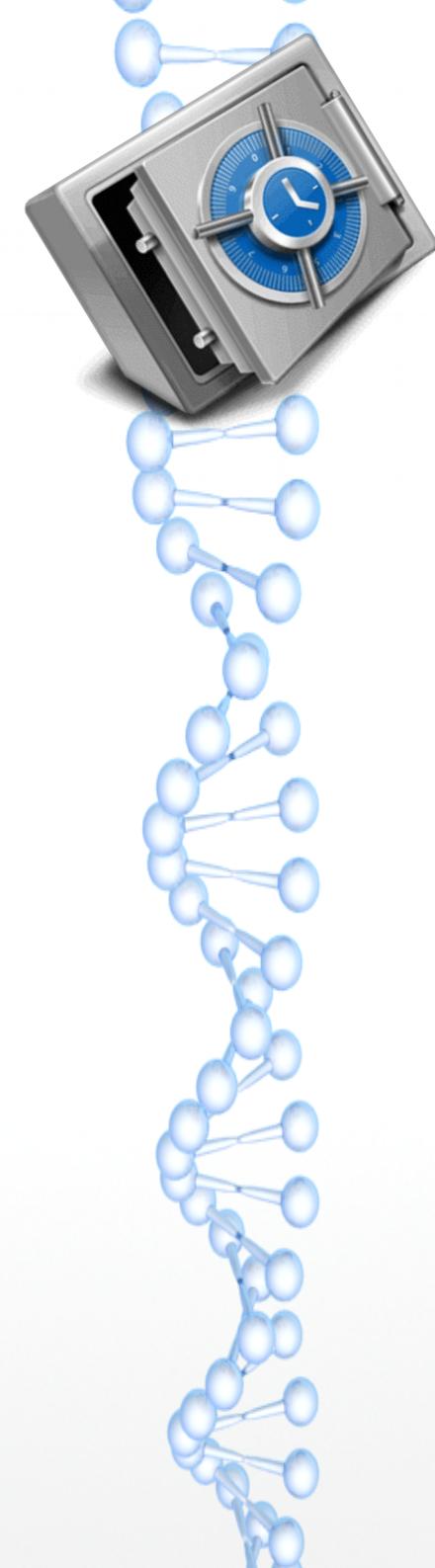
Salientamos que quem possuía créditos em seus cartões, não sofreu prejuízo algum. A empresa está tomando todas as medidas para o restabelecimento pleno do sistema, o que ocorrerá o mais breve possível e sem prejuízos aos usuários. Por fim, registramos a nossa indignação pelo ocorrido e lamentamos os transtornos a quem quer que seja.

Rio Grande, 02 de abril de 2019.



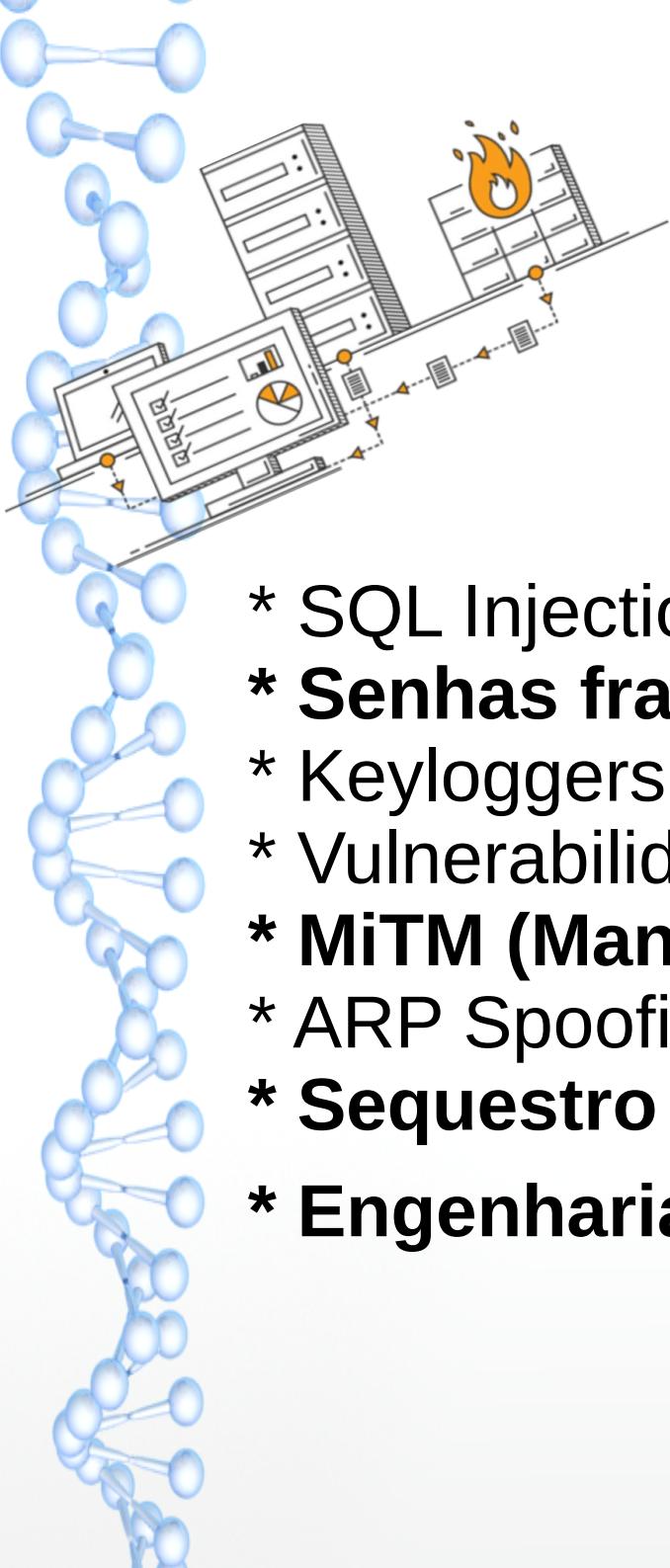
Backup – NÃO é igual a Cópia





Backup – NÃO é igual a Cópia





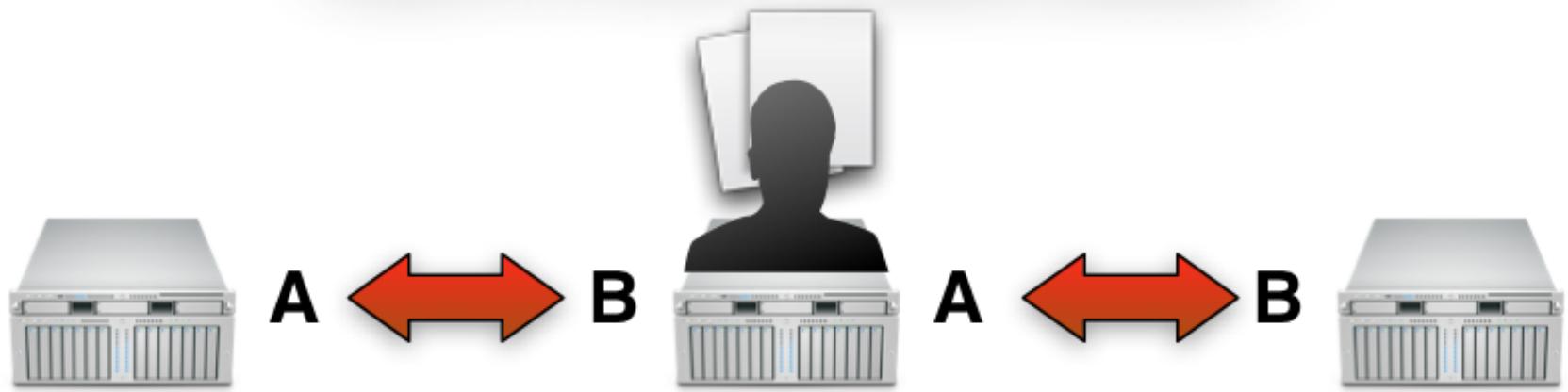
Alguns dos métodos

- * SQL Injection
- * **Senhas fracas**
- * Keyloggers
- * Vulnerabilidades novas (Zero Day)
- * **MiTM (Man in The Middle)**
- * ARP Spoofing/Poison
- * **Sequestro de DNS**
- * **Engenharia Social**

Alguns dos métodos



Man-in-the-middle attack



Algumas soluções para correção de vulnerabilidades nos roteadores





Cultura de Seg Info

- * Senhas **seguras**;
- * **Seguir** Políticas de Segurança;
- * Sempre estar **atento** as notícias;
- * Manter uma **documentação** (não TXT) de senhas/acessos;
- * **Participar/promover** eventos de Segurança da Informação;
- * Ter a TI como aliada e qualquer dúvida **solicitar** ajuda;
- * Ser um usuário de tecnologia **proativo** no que diz respeito as ameaças;
- * Sempre manter todo e qualquer **sistema atualizado** (não só antivírus) .

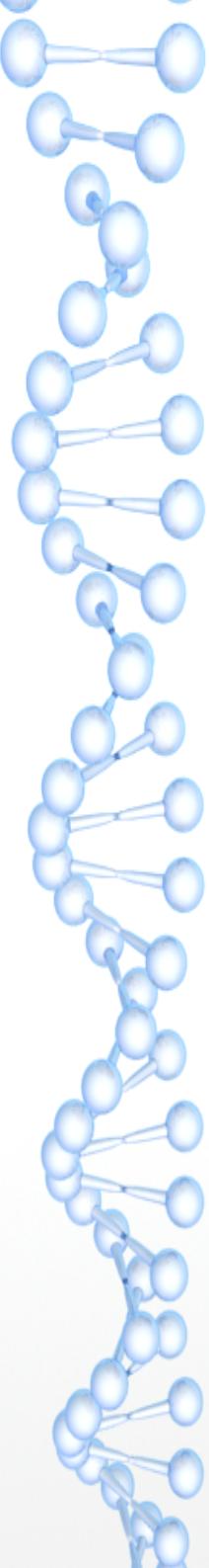
INTERNET DAS COISAS



Indicações - Livros



Indicações - PodCast



www.segurancalegal.com



Indicações - Episódios



Episódio #169 – Uso de dados por farmácias

7 de setembro de 2018

Neste episódio vamos conversar com o Davi Teófilo e a Luíza Brandão sobre a representação do IRIS acerca do uso de dados pessoais pelas farmácias.

Ajude a Segurança Legal a continuar existindo. Visite nossa [campanha de financiamento coletivo](#) e nos apoie!



Episódio #209 – Faceapp e os “Hackers” de Araraquara

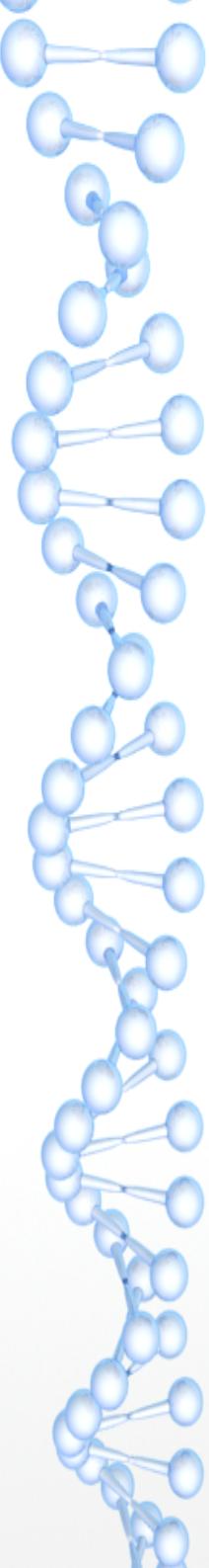
5 de agosto de 2019

te episódio falamos um pouco sobre o aplicativo Faceapp e sobre os hackers (ou seria crackers) envolvidos na invasão celulares de autoridades.

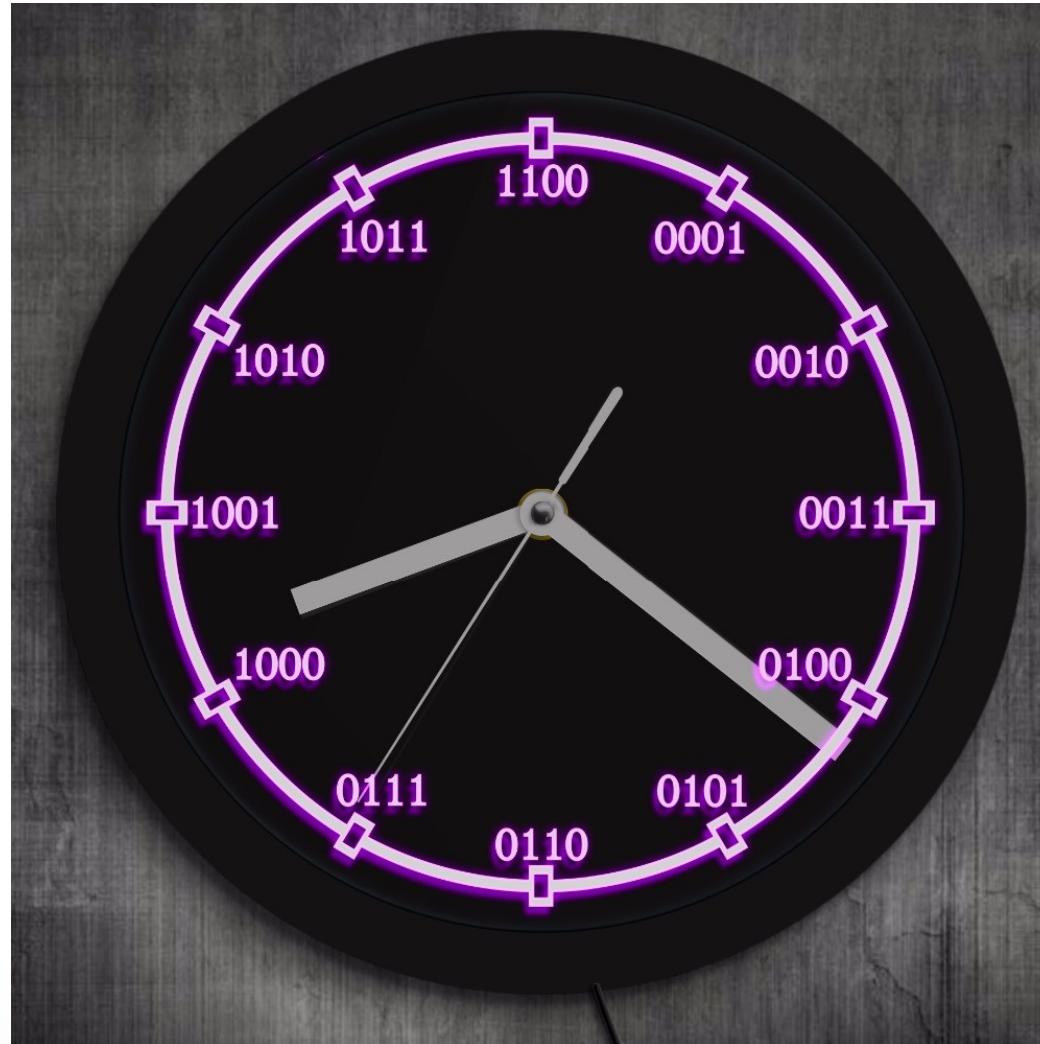


Indicações - Filmes





Temos tempo ainda?



<https://youtu.be/Zbqo7MGVEIw>





Ensino a distância

Aprendizado Contínuo

Liberdade

Colaborativismo

* **Vídeo aulas**

* **Documentações**

* **Dicas**



youtube.com/projetoroot

Perguntas?

- diegocosta@projetoroot.com.br
- www.projetoroot.com.br
- youtube.com/projetoroot
- facebook.com/projetoroot
- wiki.projetoroot.com.br

.

Diego Costa
CEO – Projeto Root