idec
Instituto Brasileiro de Defesa do Consumidor

Anti-mapa de privacidade

Feito para você não ser rastreado

Organização: Bárbara Simão e Rafael Zanatta

Pesquisa e produção de textos: Bárbara Simão, Juliana Oms, Livia Torres e Rafael Zanatta

Revisão: Rafael Zanatta

Revisão de texto: Bárbara Prado Simão

Design: Talita Patricio Martins

Supervisão: Carla Yue e Teresa Liporace

Coordenação executiva: Elici Bueno

Realização

idec
Instituto Brasileiro de Defesa do Consumidor

Idec - Instituto Brasileiro de Defesa do Consumidor

Rua Desembargador Guimarães, 21 - Água Branca

CEP 05002-050 - São Paulo-SP

Telefone: 11 3874-2150

institucional@idec.org.br

www.idec.org.br

Índice

Por que um anti-mapa?

Há quem diga que dados pessoais são o "**petróleo da era digital**". Enquanto isolados, não representam muita coisa nem possuem tanto valor, mas quando integrados e analisados em conjunto revelam perfis de consumo, de crédito, hábitos recorrentes e até padrões de personalidade.

O mercado de dados funciona assim: empresas desenvolvem modelos para prever nossos comportamentos, identificar nossas preferências e nos influenciar com propagandas especialmente direcionadas para nós, pois sabem aquilo que nos sensibiliza a partir de nosso padrão de comportamento - situação muitas vezes despercebida. Estes perfis que criam de nós podem até gerar discriminação com preços diferenciados, por exemplo, a partir do local onde realizamos a compra ou da renda obtida.

Esta situação gera sérias consequências para o modo como vivemos e nossa democracia. **Por isso, a aprovação da Lei Geral de Dados Pessoais foi tão importante: nossos dados deixarão de ser objetos passíveis de extração, pois são parte de nós e de quem somos.** Ao prever princípios éticos e direitos básicos aos cidadãos, a lei nos devolve o controle sobre todas as informações que produzimos - é como o Código de Defesa do Consumidor para as novas tecnologias.

Índice

Mas, apesar de tão importante, a lei só entra em vigor em fevereiro de 2020.

O que fazer até lá pra retomar esse controle?

Esse material foi elaborado para te ajudar! Invertendo a lógica dos mapas tradicionais, que te ajudam a **encontrar** coisas, vamos te ajudar a se **esconder**, já que nesse caso você é o tesouro para as grandes empresas. Seguindo esses passos, vai ser muito mais difícil te rastrearem e extraírem ouro pelas migalhas que você deixou pelo caminho.

Já existem inúmeras iniciativas, aplicativos e ferramentas feitas para minimizar coletas de dados. Aqui, te mostramos o caminho das pedras: filtramos conteúdos e dicas que vão te deixar menos exposto na Internet e também fora dela.

Índice

IDEC e a Lei Geral de Dados pessoais

A Lei Geral de Proteção de Dados Pessoais sancionada em 14 de agosto de 2018. **Esta é uma vitória da sociedade civil, resultado de anos de intenso debate e disputa na qual nós, do Idec, fomos um dos principais atores.**

Em 2010 e 2015 foram abertas Consultas Públicas sobre o tema pelo Ministério da Justiça, das quais resultaram milhares de contribuições e a formulação do anteprojeto de Lei apresentado pelo Executivo em 2016. Foi criada Comissão Especial na Câmara para a análise do projeto, a qual realizou onze audiências públicas, além de reuniões com diferentes setores para discussão do texto - sempre com participação ativa do Idec na construção dos debates. Acesse aqui todo nosso histórico de lutas nesta pauta.

Índice

Índice

Se preferir, clique no assunto de seu interesse para ser levado diretamente para a parte que quer ler. Ao terminar, clique em “voltar para o índice”, no canto inferior esquerdo da página, para escolher o próximo assunto.

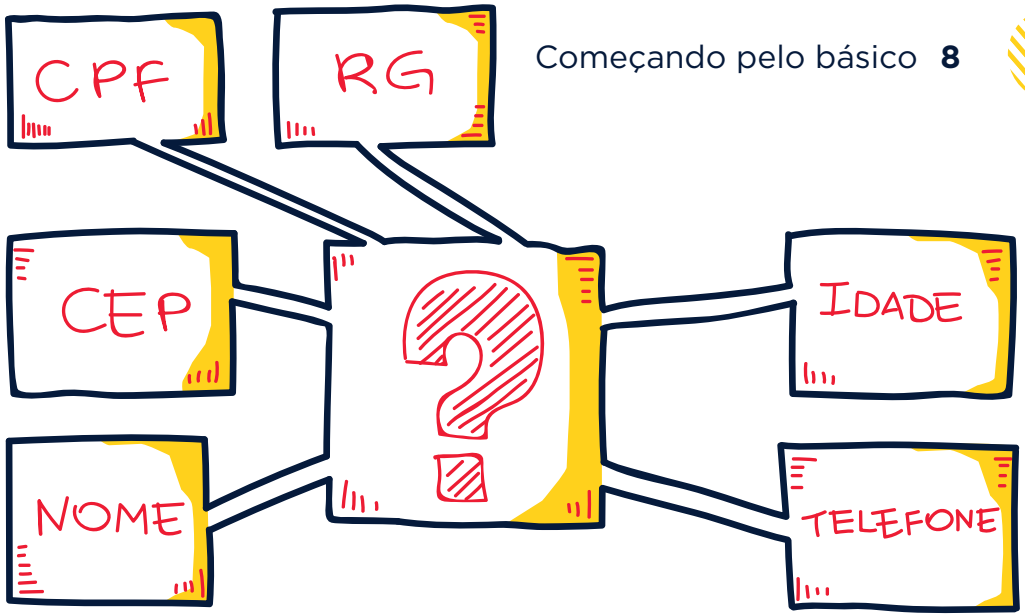
Começando pelo básico

Índice

Pergunte **por quê**

Imagine a cena: no caixa do supermercado o atendente pergunta se você não quer fazer um cadastro. “Poxa, é do lado da minha casa, sempre venho aqui. Acho que vale a pena!”, você pensa. E então uma bateria de perguntas começa: nome, CPF, endereço, se a sua casa é alugada ou própria, se você tem filhos, se eles têm alguma restrição alimentar...

Mas por que o seu supermercado precisaria saber tantos detalhes da sua vida?



Neste **vídeo** da organização de pesquisa InternetLab, este mesmo tipo de cena é retratado, porém em uma farmácia. Aos poucos, as pessoas ficam surpresas com o tom das perguntas, mas ainda acanhadas em perguntar quais os motivos da coleta de dados. O cenário muda, mas a importância do tema não: estamos acostumados a passar nossos dados nesses ambientes sem muita reflexão. Por isso, acostume-se à ideia de **perguntar por quê.**

Se achar que a informação é excessiva ou desnecessária, evite fornecê-la.

Índice

Caiu na rede é peixe

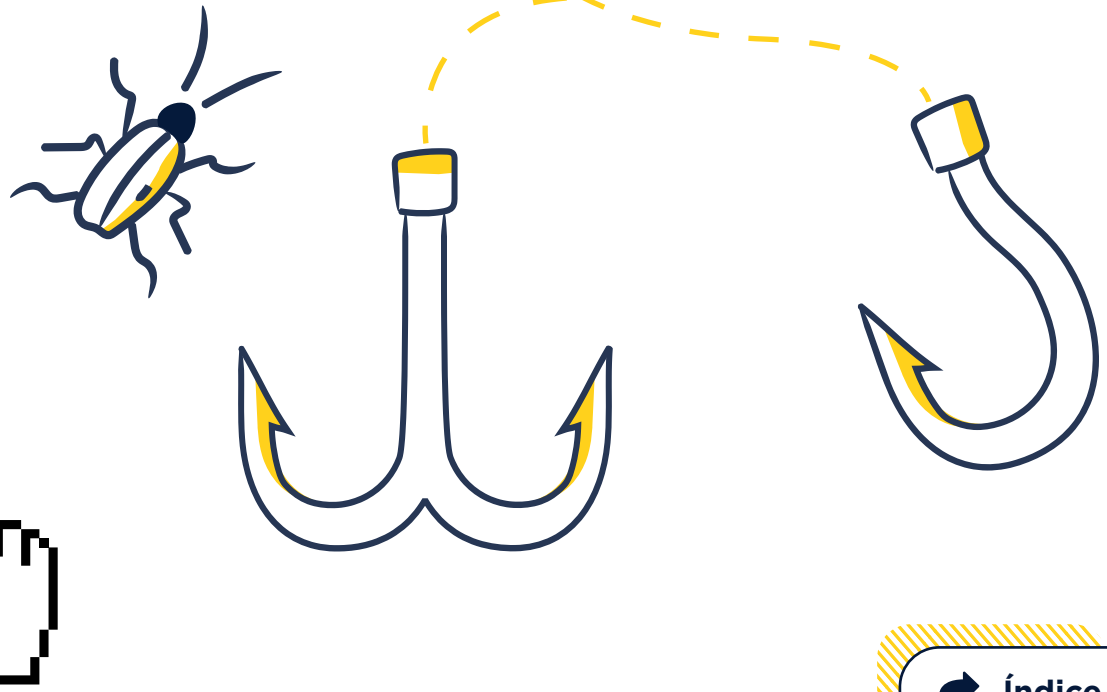
(ou: o perigo de sair clicando em qualquer coisa)

Uma consequência direta de vazamentos massivos de dados pode ser o impacto de códigos maliciosos (malwares) no seu computador.

Por exemplo: se um vazamento de dados ocorrer na sua loja de roupas favorita, pode ser que saibam quando, com qual atendente e o que você levou na sua última compra.

O QUE É UM MALWARE?

São programas desenvolvidos para executar ações danosas em um computador ou celular. É um termo genérico que inclui o vírus, spywares, dentre outros códigos maliciosos. O spyware é um tipo de código espião projetado para monitorar e enviar as informações coletadas para terceiros. E o adware, por sua vez, é projetado especificamente para apresentar propagandas.



Índice

Com essas informações tão particulares sobre você, **fica fácil elaborar uma mensagem capaz de te enganar e o direcionar a algum link malicioso**, que pode acabar instalando um vírus ou ou até mesmo um dispositivo capaz de “espiar” a sua navegação.

Este tipo de fraude é conhecido como **phishing** - uma analogia criada para a palavra “pesca” em inglês, já que eles dão a isca para tentar pescá-lo.

Por isso é tão importante que as empresas notifiquem os consumidores em casos de falhas de segurança detectadas em seus sistemas. Mas além disso, é importante desconfiar de qualquer mensagem ou e-mail de desconhecidos que se passem por empresas ou requeiram alguma informação pessoal sua.

CONSUMA INFORMAÇÃO

A Cartilha de Segurança para a Internet do Cert.br é um guia muito completo de informações, descrições e ações de segurança contra phishing e códigos maliciosos em geral. **Confira.**

Índice

Construindo senhas seguras

Saber construir senhas mais fortes é um dos primeiros passos para aumentar a sua proteção. Sua senha definitivamente não está no caminho certo se:

- É composta apenas por caracteres de um só tipo e sem caracteres especiais ou letras maiúsculas (por exemplo: “chocolate” ou “22082017”)
- É formada por sequências lógicas de números e letras (por exemplo: 12345, qwerty, 98765, abcd)
- É composta por uma data significativa (telefone, aniversário), pelo seu nome, iniciais ou qualquer informação que esteja diretamente relacionada a você
- Possui poucos caracteres

Para começar, é importante que a senha não seja pessoal, com alguma informação diretamente relacionada a você e verificada de maneira fácil por uma simples pesquisa. Mas ainda assim, é importante que ela seja prática e fácil de lembrar.

Para construir uma senha segura, tente pensar em uma frase e construí-la de maneira diferente, misturando letras, números e caracteres especiais.

Índice

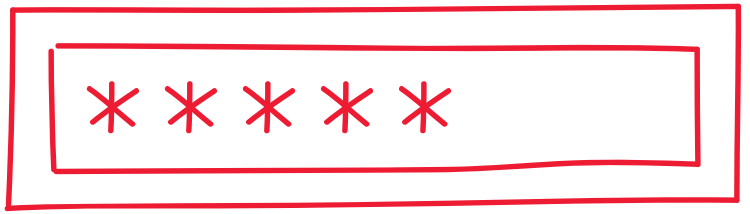
Por exemplo, a frase “o Denis torce para o Santos” pode virar “*0DeN1St0rcep/0SntS*” - uma senha muito mais forte do que apenas a frase anterior.

Vá brincando com as frases que te lembram momentos interessantes, versos de músicas, poesias, ou até mesmo trechos memoráveis do seu livro de cabeceira. Esse é o truque para criar algo marcante o suficiente para se lembrar e difícil o bastante para ficar blindado contra eventuais ataques.

Recomendamos, também, utilizar senhas diferentes para cadastros diferentes. Se você utiliza a mesma senha para tudo e ocorrer um vazamento de dados do seu e-mail, por exemplo, esta senha “já estará por aí” e poderá ser facilmente utilizada para acessar sua conta na rede social, seu banco etc.

CONSUMA INFORMAÇÃO

Sabemos que pode ser difícil de lembrar algumas senhas. Se achar melhor e isso fizer sentido para as suas necessidades, há alguns programas disponíveis que são gerenciadores de senhas. O **guia Security in a Box**, especialmente voltado para a segurança digital de ativistas e pessoas envolvidas com a defesa de direitos humanos, recomenda o programa KeePassX e traz um **tutorial** de como instalar o programa e utilizá-lo.

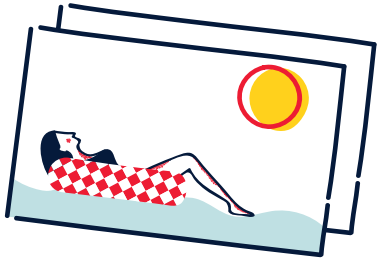


Índice

Cuidado ao andar nas nuvens

É muito comum adicionarmos arquivos na nuvem. Pode ser o Google Drive, o Dropbox, o iCloud... Qualquer site que sirva apenas para armazená-los. Normalmente, essa é uma maneira prática e acessível de acessar seus documentos a partir de qualquer dispositivo com acesso à Internet.

Mas é bom tomar cuidado: não necessariamente esta é a maneira mais segura de preservar os seus arquivos, já que esses sistemas não estão imunes a ataques e falhas de segurança capazes de colocar as suas informações em risco.



Índice

Portanto, **evite colocar na nuvem qualquer coisa que normalmente seria mantida fechada em uma gaveta com chave,** como arquivos confidenciais, cópias de documentos particulares e fotos íntimas. Neste caso, o melhor é optar por pastas dentro do seu próprio computador ou HD externo, de preferência criptografadas e com senha.

CRIPTOGRAFIA

Significa basicamente falar em códigos. De forma simples, quando falamos que um documento foi criptografado, queremos dizer que a ele foi atribuído uma sequência de números. A não ser que a chave desta sequência seja revelada, qualquer pessoa que queira acessar o arquivo ou documento não vai conseguir decifrá-lo e, portanto, acessar e entender o seu conteúdo. No exemplo abaixo, sem a informação de que A=42 e N=28, não seria possível afirmar que 422842 seria o equivalente a ANA.

A = 42
N = 28 **= ANA = 422842**

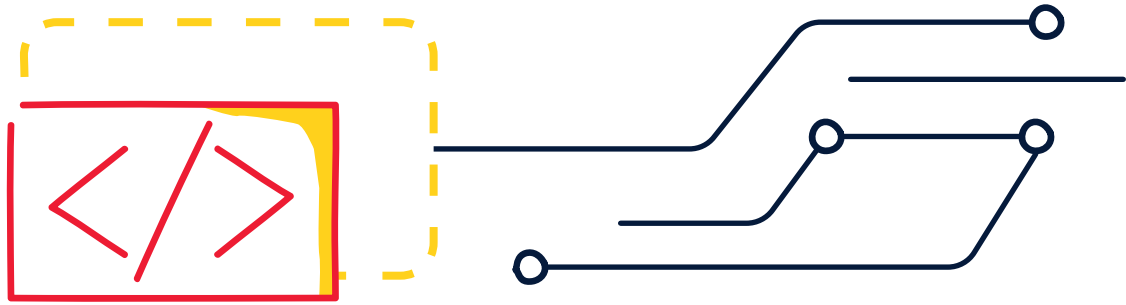
E esse assunto ainda vai longe, já que existem diversos tipos de criptografia possíveis. Se quiser saber mais, recomendamos para começar esse vídeo e essa publicação com ferramentas que podem ser utilizadas para criptografar os seus próprios arquivos.

Índice

Navegando por águas mais claras

Índice

Use navegadores mais seguros



Imagine que você está em um navio com paredes que não parecem lá muito firmes e que, dentro dele, não há qualquer janela para ver o exterior. Você teria coragem de arriscar-se e ir para o mar?

A analogia funciona para se pensar a nossa navegação pelas páginas de Internet. Elas são a fonte mais frequente de infecções no computador por códigos maliciosos, e por isso é importante que você navegue de maneira segura.

O QUE É CÓDIGO ABERTO?

Em linhas gerais, ser de código aberto significa que o código fonte de um programa pode ser acessado por qualquer pessoa, permitindo ou não sua modificação e redistribuição.

Recomendamos o uso do Mozilla Firefox, um navegador livre, de código aberto, que possibilita a utilização de vários complementos/extensões para deixar a sua navegação mais segura e privada. Para o celular, o equivalente é o **Firefox Focus**.

Índice

Para instalar o Firefox

1. Vá para o site do Firefox: https://www.mozilla.org/en-US/firefox/new/

2. Clique em Download Gratuito

3. Uma vez que tenha feito o download, clique duas vezes sobre o arquivo baixado. Uma tela de Controle de Conta de Usuário irá aparecer, perguntando “Deseja permitir que este aplicativo faça alterações no seu computador?”. Clique em Sim.

O QUE É SOFTWARE LIVRE?

É um sistema operacional totalmente livre, que pode ser copiado, usado, modificado e redistribuído de acordo com as necessidades de cada usuário.

O Firefox é de código aberto, porém existe uma polêmica se é ou não um software livre. O navegador abre o código fonte e permite sua modificação e redistribuição, no entanto sua licença exige que as modificações devem usar outro nome, para proteger o nome da empresa. Assim, embora o próprio Firefox se afirme como software livre, há quem discorde.

O QUE É PLUGIN?

Todo programa, ferramenta ou extensão que se encaixa a outro programa principal para adicionar mais funções e recursos a ele.

Índice

Também recomendamos as seguintes extensões:

HTTPS Everywhere: facilita a conexão com segurança a sites que permitem o uso de criptografia, automaticamente requerendo uma conexão criptografada a eles. **Instale aqui**.

Privacy Badger: bloqueia publicidade espiã e rastreadores invisíveis. **Instale aqui**.

No Script: faz com que JavaScript, Java, Flash e outros plugins só possam ser executados por websites confiáveis. **Instale aqui**.

Click&Clean: deleta seus dados pessoais armazenados no disco rígido do seu computador pelo navegador e armazenados no seu histórico de internet. Quando você entra em um website, ele pode acessar estes dados armazenados, como informações do cartão de crédito ou registro de saúde, sendo, portanto, importante fazer uma limpeza regularmente. **Instale aqui**.

Índice

Navegar em modo anônimo serve pra quê?

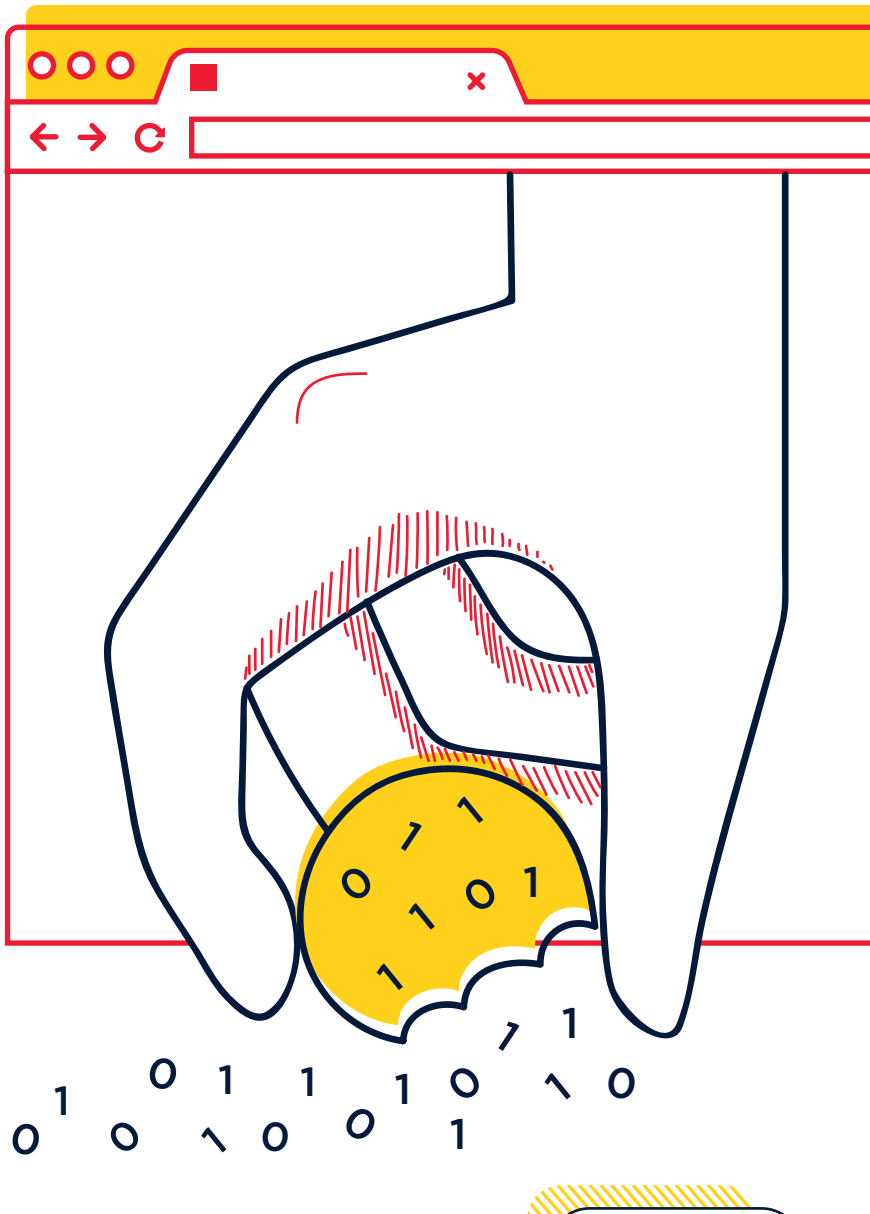
Sempre que navegamos na Internet, uma série de informações são armazenadas em nosso computador. Elas possibilitam que, ao entrar novamente em um mesmo site, tudo seja carregado de maneira mais rápida. Além disso, todas as páginas visitadas ficam registradas no histórico de navegação.

O modo anônimo permite a navegação sem deixar esses rastros armazenados no próprio computador (no disco rígido e no histórico). E se o site exigir algum armazenamento de dados, as informações serão retidas apenas temporariamente, sendo eliminadas assim que a janela for fechada.

Ou seja: **a navegação anônima é especialmente útil para manter a sua privacidade caso o computador utilizado seja de uso compartilhado.** É o caso ideal para quando você acessa seu e-mail ou redes sociais de uma lan house, por exemplo. Mas continua sem impedir rastros de navegação deixados na própria internet, em servidores e roteadores, que ainda podem rastrear outros dados como a sua localização a partir do seu número IP. Por isso, continua sendo importante instalar os complementos e extensões mencionados acima no seu navegador padrão.

Índice

No meio do caminho, tinha um cookie



Cookies são como “escreventes digitais”, que registram todos os seus rastros deixados na internet. Esses pacotes de informação ficam armazenados e são reutilizados quando um mesmo site é acessado. São eles que possibilitam a autenticação automática no seu e-mail e o registro de outras preferências de navegação, por exemplo.

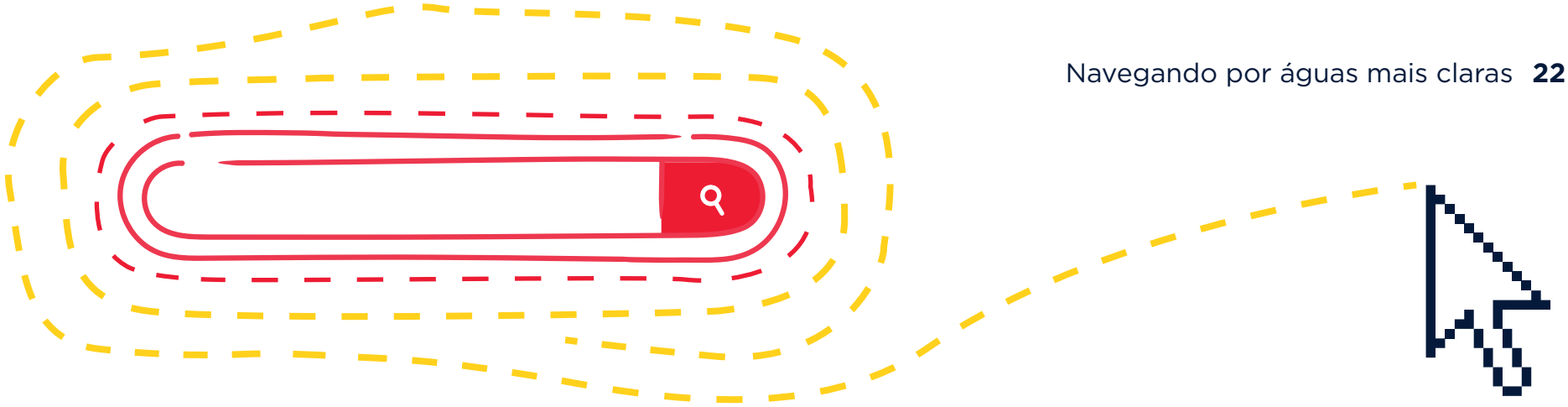
Tudo isso oferece alguns riscos, já que **os cookies permitem identificar alguns hábitos do usuário e até explorar vulnerabilidades do seu computador.** Mas também não são totalmente dispensáveis: sem eles a navegação em alguns sites fica inviável, comprometendo a sua experiência.

Índice

Para lidar com isso, você pode seguir algumas dicas da Cartilha do Cert.br:

- Ao usar um navegador Web baseado em níveis de permissão, como o Internet Explorer, procure não selecionar níveis de permissão inferiores a “médio”;
- Em outros navegadores ou programas leitores de e-mail, configure para que, por padrão, os sites não possam definir cookies e crie listas de exceções, cadastrando sites considerados confiáveis e onde o uso de cookies é realmente necessário, como Webmails e de Internet Banking e comércio eletrônico;
- Caso você, mesmo ciente dos riscos, decida permitir que por padrão os sites possam definir cookies, procure criar uma lista de exceções e nela cadastre os sites que deseja bloquear;
- Configure para que os cookies sejam apagados assim que o navegador for fechado;
- Configure para não aceitar cookies de terceiros (ao fazer isto, a sua navegação não deverá ser prejudicada, pois apenas conteúdos relacionados a publicidade serão bloqueados);
- Utilize opções de navegar anonimamente, quando usar computadores de terceiros (ao fazer isto, informações sobre a sua navegação, incluindo cookies, não serão gravadas).

Índice



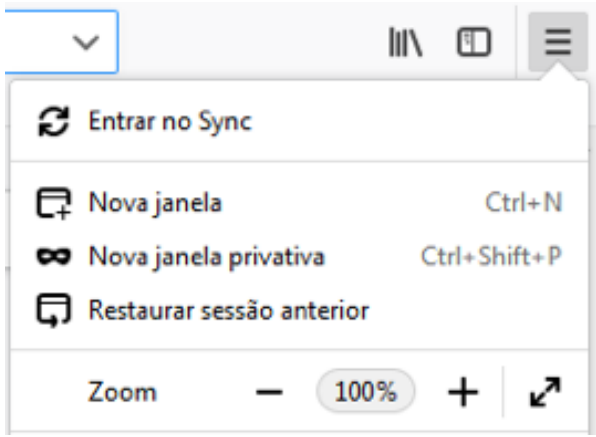
Mecanismos de busca **que sabem demais**

Seus mecanismos de busca, como Google ou Yahoo, podem desenhar um perfil a partir das pesquisas realizadas e direcionar o resultado das buscas e as publicidades expostas. Dê uma olhada **aqui** pra ver como o Google personaliza os anúncios para você.

Para fugir disso, a ferramenta de busca **DuckDuckGo** é interessante porque ela não irá rastrear, perfilizar ou compartilhar suas informações pessoais com terceiros.

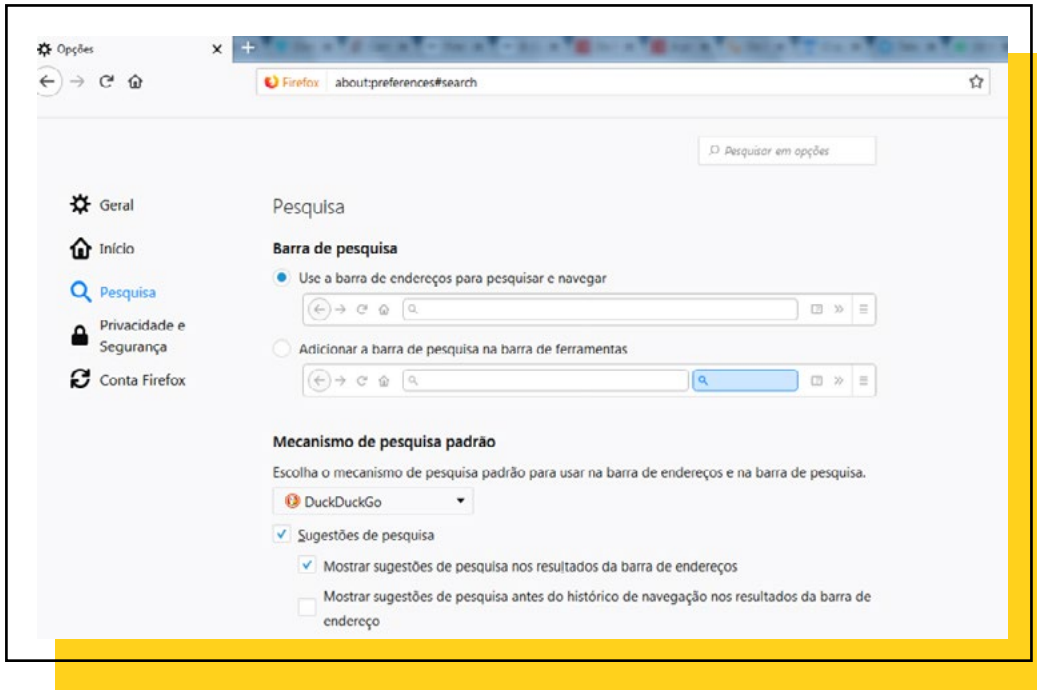
Se quiser defini-la como sua ferramenta padrão, siga os passos abaixo:

1. Selecione [Opções] ou [Configurações] no menu do topo direito do seu navegador.



Índice

2. Na tela de configurações/opções, clique em [pesquisa] ou [Gerenciar mecanismos de pesquisa], e em seguida escolha o DuckDuckGo como mecanismo padrão.



Outras ferramentas de busca que também privilegiam sua privacidade são a **StartPage**, a **Ixquick** e o **Disconnect.**

Não quer se afogar no meio de tanta publicidade?

O **AdBlock** é uma extensão de código aberto e funciona para a filtragem de conteúdo e anúncios, evitando que eles sejam exibidos no seu navegador. Além de evitar propagandas indesejadas, deixa sua navegação mais rápida, já que certos anúncios sequer são carregados. É atualmente a extensão mais popular do Google Chrome. Instale **aqui**.

Índice

No reino das Redes Sociais

É muito fácil perder a cabeça no reino das redes sociais. Afinal, elas já são programadas para te segurar o maior tempo possível dentro delas. Sabe quando você entra em uma rede social para procurar uma mensagem específica e, quando se dá conta, já gastou uns bons minutos apenas vendo memes sobre política e nem lembra mais porque foi parar ali? Nada é por acaso.

E quanto mais tempo você fica lá, mais dados elas conseguem sobre você.

Mas sabemos o quanto é inevitável escapar e deixar de utilizá-las. Então você pode seguir algumas dicas para ter mais controle sobre o que essas empresas podem saber sobre você e também entender por que elas te mostram certas coisas.

Índice

Controles de privacidade

Muitas vezes é possível controlar suas permissões em relação à privacidade e a anúncios publicitários nas próprias configurações da sua conta.

No caso do Facebook, é possível fazer tudo isso por dois caminhos:

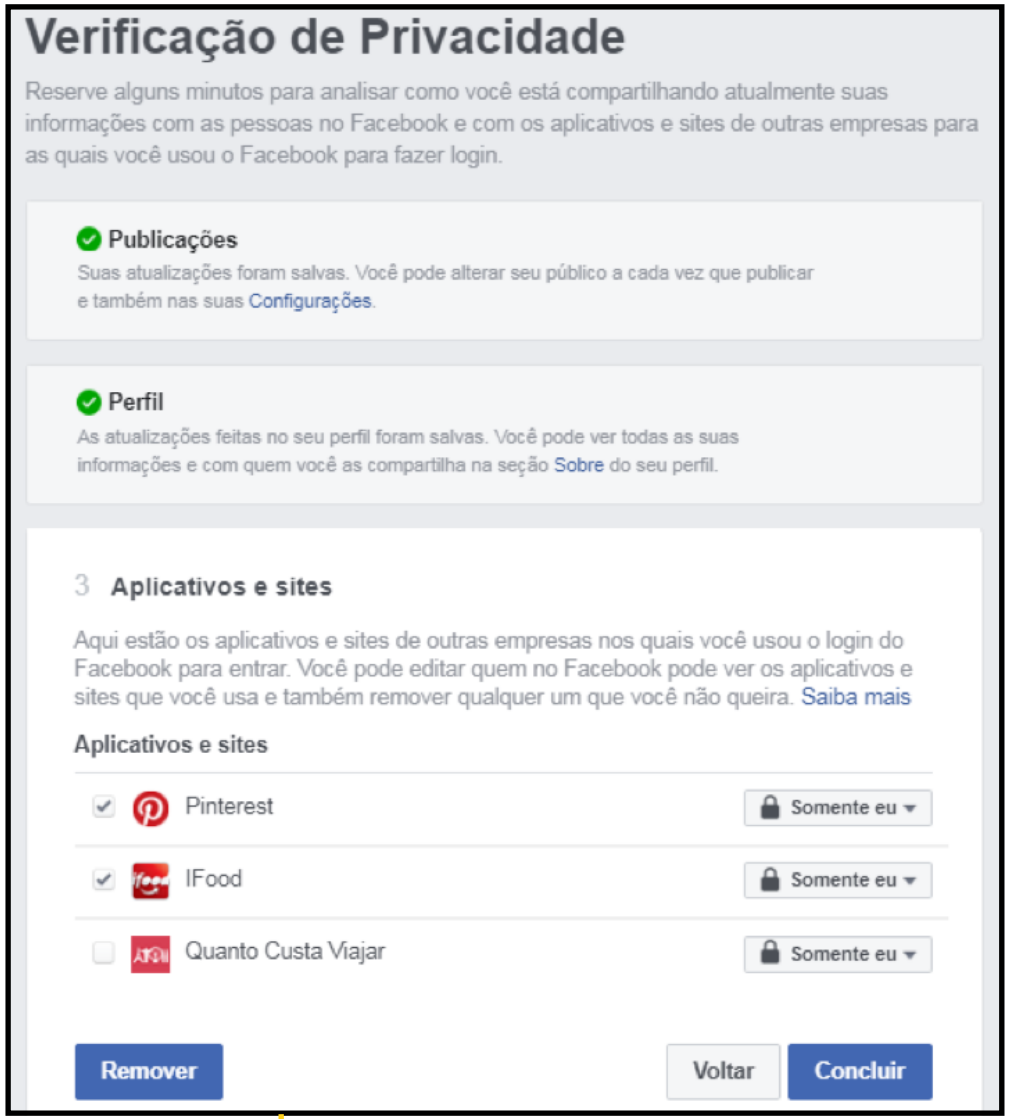
1. O atalho - verificação de privacidade do próprio facebook

Índice

O Facebook disponibiliza um caminho mais simples de verificação de privacidade, acessível por meio daquele ponto de interrogação no canto superior direito da tela.

Por meio dele, é possível ajustar algumas coisas básicas: publicações, perfil e permissões para aplicativos e sites.

Caso você não queira mais dar permissão a um aplicativo específico, selecione-o e clique em “remover”. Depois de ter feito isso, é só concluir o processo.



Índice

2. O caminho mais seguro

É possível encontrar todos os controles de ajuste de privacidade, segurança da conta e exibição de anúncios por meio do caminho https://www.facebook.com/privacy/

Preste atenção especialmente nos controles sobre reconhecimento facial, configurações de localização e preferências de anúncios.

O primeiro permite que o facebook te identifique em fotos ou vídeos utilizando mecanismos de inteligência artificial. O segundo mostra todo o seu histórico de localização quando você usou o facebook como aplicativo no celular.

Já o tópico de preferências de anúncios permite que você controle que tipo de informações podem ser vistas por terceiros que desejam direcionar propagandas diretamente a você - e até mesmo desativar a exibição de anúncios com base nas suas preferências pessoais.

Índice

Qualquer que seja a rede social, é importante explorar!

Normalmente essas permissões ficam meio escondidas em algum lugar das configurações de privacidade da conta. Mas faça o exercício de caçá-las! Assim, não importa qual seja a rede social, você sempre estará protegido.

FUZZIFY.ME

Também é possível controlar exibições de anúncios para o seu perfil com a ferramenta **Fuzzify.me**, desenvolvida pela Coding Rights. A extensão, que pode ser instalada no seu navegador, ajuda a confundir os algoritmos do Facebook e a obter transparência sobre como o direcionamento de publicidade funciona. Veja o **vídeo** explicando!

TWITTER E YOUTUBE

Para facilitar a sua vida, nós já descobrimos os caminhos do Twitter e da Google (que serve para qualquer conta vinculada à empresa, como o Youtube). Mas se conseguir achar primeiro, ponto pra você!

Índice

Quem conta um conto aumenta um ponto:

o impulsionamento de campanhas em tempos de eleições

Já não é mistério que candidatos utilizam redes sociais para realizar propaganda política no período eleitoral. As táticas variam: pode ser pela utilização de robôs sociais, que são perfis falsos que apenas replicam em massa informações dos candidatos que "apoiam" ou por impulsionamento de publicações, em que uma certa quantia é paga para o impulsionamento de um conteúdo específico nas redes, dentre outras possibilidades. Esse direcionamento é sempre feito com base nos seus dados, levando em conta suas características e perfil pessoal - e mesmo suas características psicológicas, como ocorreu no caso da Cambridge Analytica.

O que muita gente ainda não sabe, em razão de critérios pouco transparentes, é **como isso é realizado, com base em que informações e a quem atinge.**

Para entender melhor como isso ocorre, você pode usar uma ferramenta desenvolvida pelas organizações de pesquisa InterneLab e WhoTargets.me, que funciona pelo menos para o Twitter e Facebook: chama-se **Você na Mira**. Este projeto, além de te dar informações mais claras sobre quem direciona propaganda a você e porquê, gera também uma análise agregada, que faz entender a dimensão do impulsionamento de campanha para cada partido.

Índice

Retomando o controle **sobre o seu celular**

Índice

O seu celular é um instrumento capaz de te monitorar a todo instante. Vejamos:

- Sensores corporais podem identificar a quantidade de passos que você dá em um dia, a sua velocidade, saber se você está andando de carro, ônibus ou bicicleta.
- Dispositivos de localização são capazes de identificar com precisão os locais onde você esteve ao longo do dia e os horários exatos de chegada e partida.
- Dependendo das permissões dadas ao uso de microfone, pode ser que ele acabe registrando a sua voz e conversas mesmo que você não tenha percebido.

Isso, claro, depende da maneira como você usa o seu dispositivo e das permissões que dá a cada aplicativo instalado nele. O problema é que, normalmente, as configurações de origem dos aplicativos instalados já vêm permitindo uma coleta massiva e exagerada de dados - muitas vezes desnecessários ao seu funcionamento.

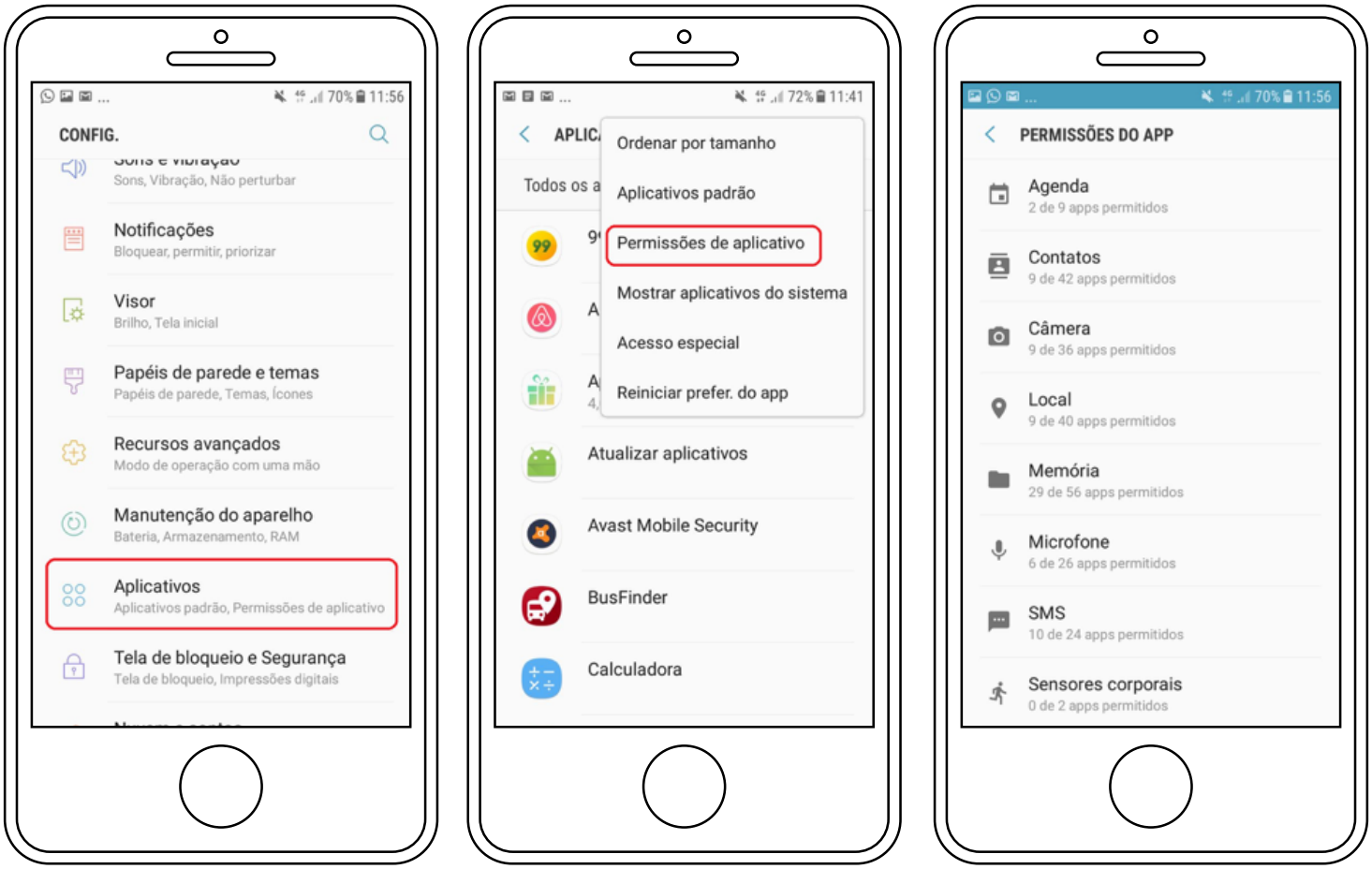
Por que o seu aplicativo de banco iria precisar de acesso aos sensores corporais? Por que o seu aplicativo de corrida teria acesso ao seu microfone ou às suas fotos?

Mas nem tudo está perdido: é possível retomar o controle sobre suas informações mudando apenas algumas configurações no seu celular. Assim, você pode controlar que tipos de dados sobre você são compartilhados para cada aplicativo.

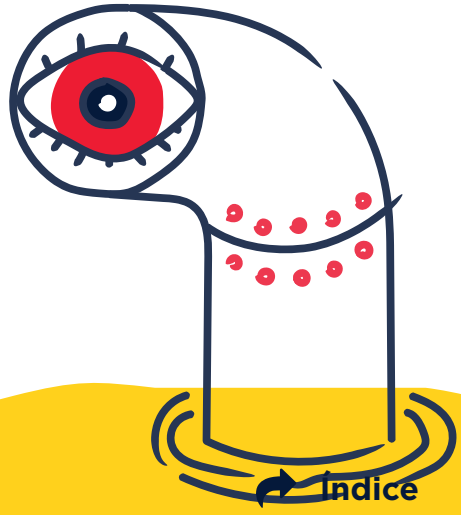
Índice

O caminho do sistema Android:

> Configurações > Aplicativos > Permissões dos aplicativos > explore!



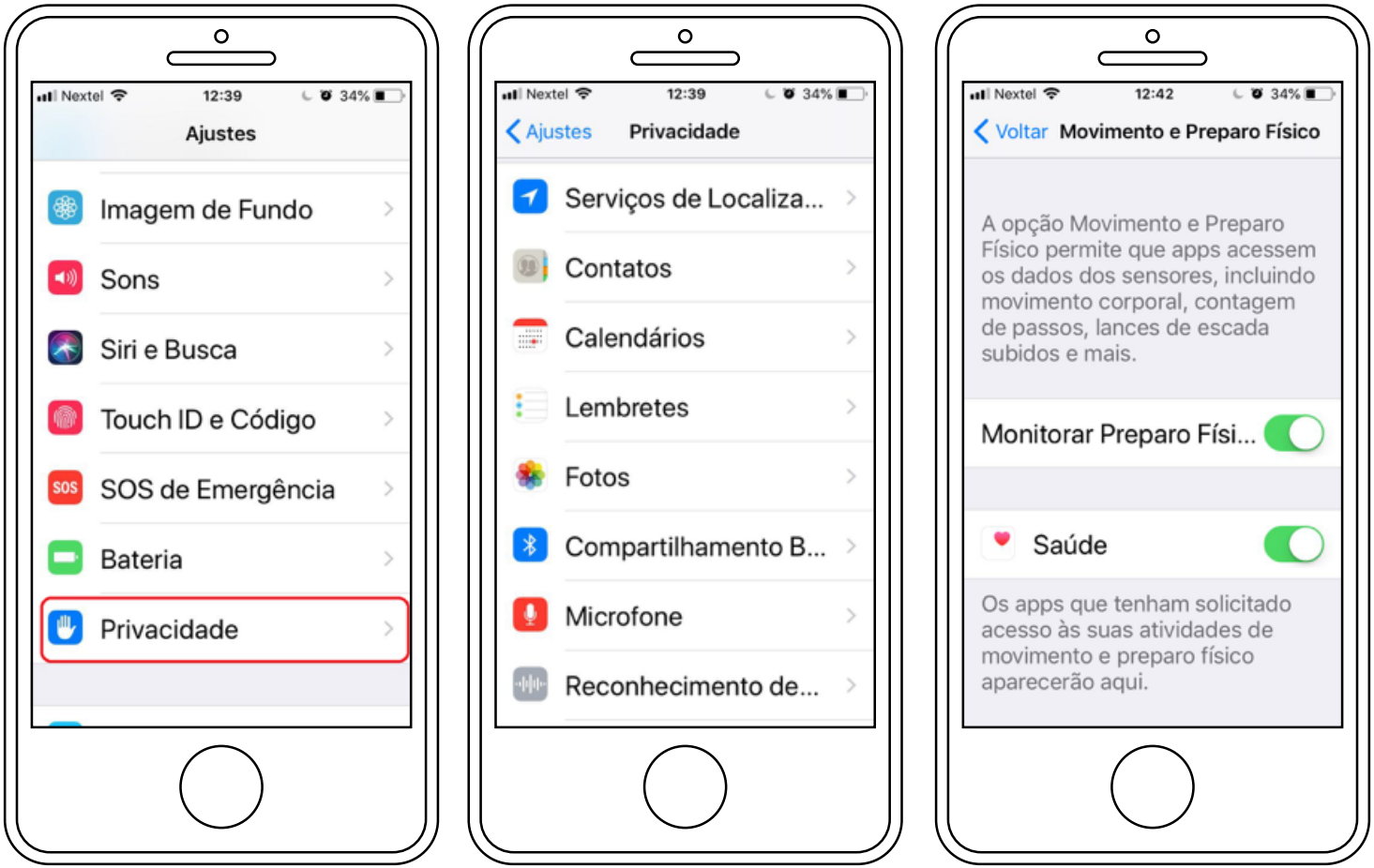
Observação: infelizmente, existem alguns aparelhos mais antigos em que não é possível alterar esse tipo de configuração.



Índice

O caminho do sistema IOS:

> Ajustes > Privacidade > explore!



Questione e investigue o quanto de informações sobre você é enviada para terceiros. Indicamos que você você permita apenas a coleta daquele mínimo de dados necessário para o que você precisa. **E lembre-se de deletar os apps não utilizados!**

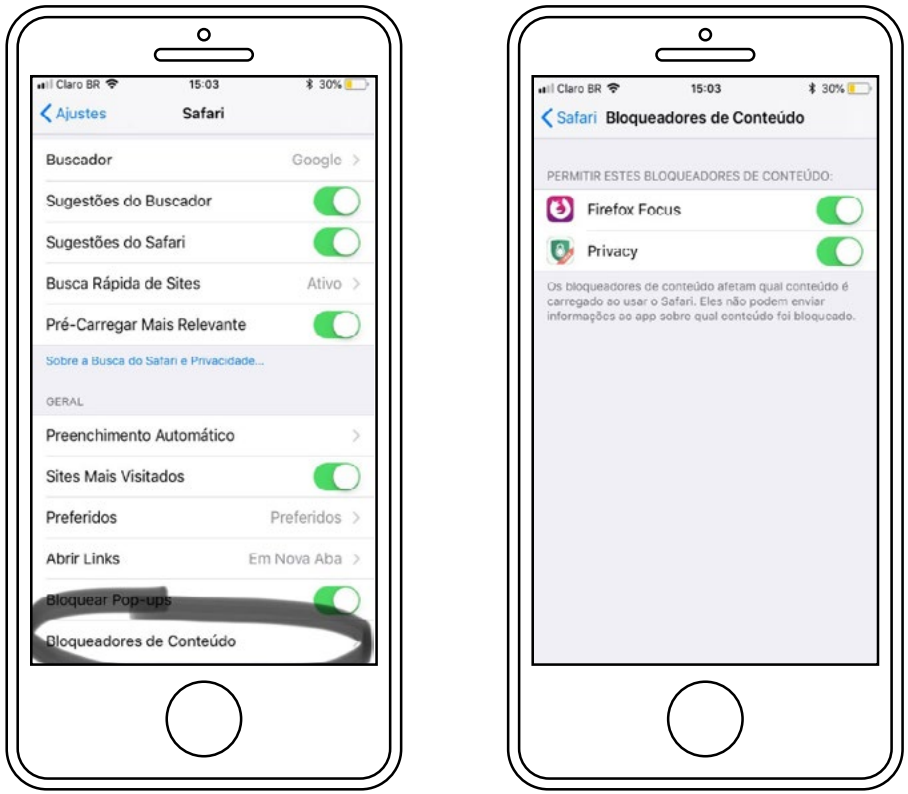
Índice

Dica boa: Disconnect

O Disconnect é uma extensão em código aberto, para Android e iPhone, que impede rastreadores que querem coletar seus dados de forma não consensual e permite que você veja quais websites estão querendo rastrear seus dados.

Em 2014, o Disconnect foi banido da Google Play Store, retornando à loja após protestos de ONGs como a EFF.

Para utilizá-lo, você deve fazer o download do aplicativo e abrir “Configurações”. Selecione o navegador utilizado e depois clique em “Bloqueadores de Conteúdo”. Habilite a opção “Privacy” (Disconnect).



Não ignore o antivírus

Embora o risco contrair vírus no celular seja menor que no computador, ainda há a possibilidade do seu dispositivo ser infectado. Por isso, é igualmente importante a instalação de um antivírus no celular.

Índice

idec
Instituto Brasileiro de
Defesa do Consumidor

@idec

idecbr

idecbr

defesadoconsumidor

instituto-brasileiro-de-defesa-do-consumidor

Índice