Global Encryption Coalition

Tradução por

Instituto de Pesquisa em Direito & Tecnologia do Recife

Guia de Criptografia para Pais e Mães

A criptografia pode parecer coisa de filme de espião, mas todos nós dependemos dela para ficar seguros. Você pode se surpreender com a frequência que ela afeta sua vida. Inclusive, você está usando criptografia agora mesmo.

Como a criptografia protege você e seus entes queridos?

Toda vez que você digita uma senha, escaneia seu smartphone para pagar um café, envia uma foto de seu filho marcando um gol para seus pais ou usa um relógio fitness para monitorar seu recorde pessoal, a criptografia ajuda a garantir que ninguém mais possa ver essas informações. Quando seus dados são criptografados, isso significa que eles são embaralhados, seja quando estão em movimento, seja quando estão armazenados em algum lugar. Isso torna mais difícil para os hackers interferirem em sua vida financeira, roubarem sua identidade ou obterem aquelas fotos que você queria que fossem vistas por aquela pessoa. É por isso que é tão importante tomar algumas medidas para garantir que seus dispositivos, aplicativos e serviços estejam realmente utilizando criptografia. Você está vendo este site graças aos dados que estão sendo enviados entre seu dispositivo, seu navegador e uma série de conexões, servidores e computadores. Mas por conta do site usar uma ferramenta criptografada chamada HTTPS, fica mais difícil para qualquer pessoa saber que você está lendo sobre como usar a criptografia.

PAIS E MÃES

Monitores de bebês

Tenha certeza de que esses sussurros do bebê são só para você

A casa mais inteligente é aquela criptografada. Aprenda a escolher os mais seguros monitores para bebês e dispositivos domésticos conectados

Os monitores para bebês oferecem tranquilidade e dão a você a chance de intervir rapidamente se seu filho tiver uma emergência de saúde ou apenas precisar de conforto após um pesadelo. Eles permitem que você acompanhe a atividade do seu bebê em outro cômodo ou fora de casa.

Mas se o seu monitor estiver conectado à Internet, esse "outro cômodo" pode ser quase qualquer lugar e talvez você não saiba quem está nele.

Quando outra pessoa pode monitorar seu bebê

Pais e mães usam monitores para bebês desde a década de 1930. Mesmo nessa época, por vezes os aparelhos captavam sinais de dispositivos próximos que estavam na mesma frequência. Não era um fantasma cantarolando, mas sim seu vizinho cansado cantando "brilha, brilha estrrelinha" pela milésima vez às 2 da manhã (quem viveu, sabe).

Os dispositivos atuais são mais sofisticados, com vídeo e áudio de alta qualidade, cancelamento de ruído e até microfone bidirecional.

Alguns podem se conectar ao WiFi de sua casa, o que significa que você pode acessá-los mesmo fora de casa. Então, quando a babá ligar para dizer que não consegue fazer com que seu filho ansioso se acalme, você também pode cantar mil versões de "Cai, cai balão", direto daquele jantar romântico em um restaurante. Só que estar conectado à Internet traz um risco adicional. A ponta emissora é um microfone e uma câmera dentro de sua casa, fisicamente perto de seu filho. E que, provavelmente, está ligado o tempo todo.

Ela funciona transmitindo um sinal enviado pela Internet para um servidor a partir do seu telefone. Se isso não for seguro, pode significar que alguém malicioso também pode ouvir você cantar "Bom dia, o sol já nasceu lá na fazendinha". Essa pessoa poderia usar a capacidade de escuta para coletar suas informações pessoais, ver como você se movimenta pela casa ou colocar seu bebê em risco.

Você deveria sequer usar uma babá eletrônica? Talvez você não devesse nem sair para jantar... Mas calma! Não cancele ainda sua reserva de jantar.

Calma: veja por que você não precisa entrar em pânico
Os dispositivos domésticos conectados não são inerentemente perigosos, mas é importante conhecer algumas maneiras de evitar escutas indesejadas. Mesmo que suas comunicações ocorram através dos servidores dos fabricantes, eles não deveriam assistir ou ouvir o que está acontecendo ou acessar os dados enviados.

Para garantir isso, é importante escolher um modelo de babá eletrônica ou dispositivo doméstico conectado que possua tecnologia de criptografia ponta-a-ponta. Isso protege a conexão e mantém o sinal – e as músicas de ninar – apenas entre você e seu bebê (e o resto do restaurante). E quem sabe quando você chegar em casa, seu bebê tenha descoberto Mundo Bita.

O que recomendamos
1. Escolha dispositivos que ofereçam criptografia, de preferência, ponta-a-ponta. Reserve alguns minutos para revisar as especificações detalhadamente. Se for comprar em uma loja física, pergunte a um especialista caso não encontre os detalhes técnicos.

2. Se o dispositivo tiver algo chamado “assistente inteligente”, ele provavelmente será iniciado por meio de uma palavra de ativação. Ele está sempre atento a essa palavra, o que significa que pode ser “acordado” por acidente e começar a ouvir tudo em busca de comandos. Geralmente não é possível saber para onde vão essas comunicações de voz ou como serão armazenadas. Desligue o assistente de voz quando não precisar dele imediatamente. (O mesmo vale para assistentes de voz como Siri e Google Home em dispositivos móveis.)

3. Verifique e exclua periodicamente todas as gravações de dispositivos como Alexa, Siri ou Google Home.

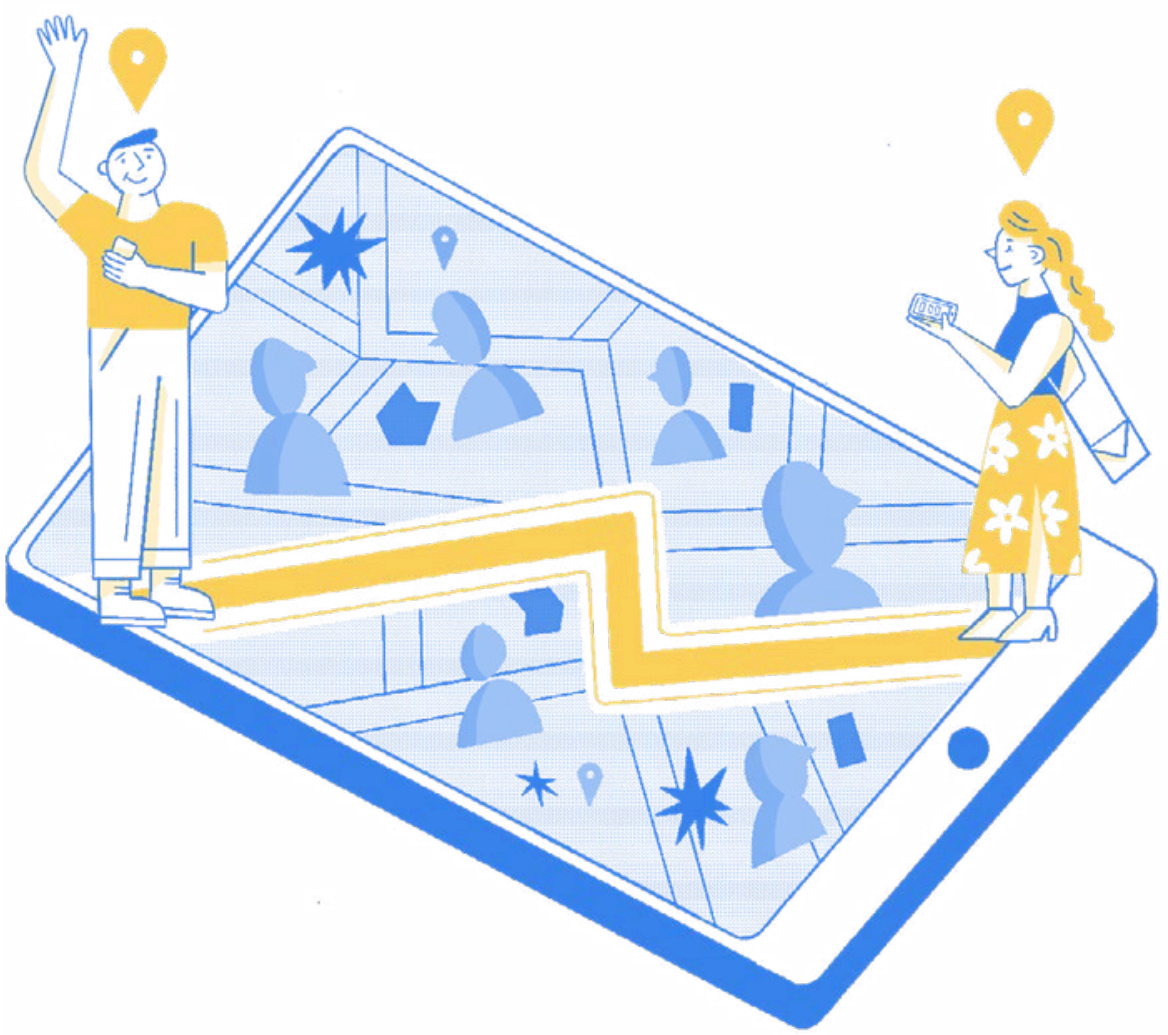
4. Se você não precisar do acesso remoto, considere desabilitá-lo.

5. Altere a senha padrão.

PAIS E MÃES

Compartilha-mento de localização

Garanta ninguém mais possa saber sua localização



Compartilhar a localização é uma maneira conveniente de manter crianças e adolescentes seguros. Descubra como ter certeza de que você não está compartilhando isso com as pessoas erradas.

Quando as crianças são (quase) adolescentes, você pode querer que elas digam mais de três palavras para você, on-line ou off-line. Você espera que elas realmente estejam dormindo na casa daquele amigo ou daquela amiga.

O compartilhamento de localização é útil para ajudar os jovens a exercer a sua crescente autonomia sem acabar com o rolê deles. Eles ainda querem que você vá buscá-los... só que na esquina.

Mas com quem mais eles estão compartilhando sua localização?

Quando compartilhar a localização não é segredo

Mais do que tudo (exceto dados móveis ilimitados), os jovens querem ir a festas e sair com os amigos sem você ficar atrás deles. Antigamente, você tinha que incomodá-los para saber um endereço ou pedir aos pais dos amigos deles que lhe dessem as direções. Mas graças aos recursos de compartilhamento de localização em seus telefones, eles podem simplesmente enviar onde estão para que você os encontre.

Eles podem até usar o compartilhamento de localização entre si. Todos nós lembramos - ou éramos - o amigo que saiu bravo de um rolê e se arrependeu logo depois. Compartilhar a localização os ajuda a se encontrarem novamente quando tudo estiver perdoado e esquecido. Esse uso também é comum entre grupos de colegas, principalmente mulheres, para compartilhar sua localização quando vão a um encontro com alguém.

Seu filho adolescente pode estar sendo rastreado ao andar por aí, jogar um jogo baseado em localização ou postar nas redes sociais. Sem você saber, alguns desses aplicativos podem rastrear locais, criar históricos de localização e salvá-los em registros.

Se esses dados não são criptografados ou são compartilhados publicamente, eles podem revelar rotas regulares entre casa, escola, trabalho ou amigos, ou mostrar a localização de uma pessoa em um local confidencial, sem que ela saiba. A última coisa que seu filho deseja é que o valentão da escola saiba aonde ele vai todas as semanas.

Usado com sabedoria, o compartilhamento de localização pode ser útil, conveniente e seguro. É por isso que é importante ter algumas táticas para evitar a exposição de informações a agentes maliciosos ou predadores.

Calma: veja por que você não precisa entrar em pânico

Quando se trata de compartilhamento de localização, os usuários geralmente têm bastante controle. Você pode desativar esse compartilhamento para a maioria dos serviços ou usá-lo apenas quando o aplicativo estiver em uso. Escolher serviços criptografados significa que apenas quem você permite pode saber onde você está ou esteve.

Você ainda pode compartilhar sua localização para encontrar seus amigos, pegar seu filho ou fazer longas caminhadas - só que diretamente com as pessoas e grupos que você escolher.

O que recomendamos

1. Use serviços criptografados que permitam compartilhar sua localização com segurança.
2. Desative todos os recursos de compartilhamento de localização nos aplicativos que você usa. Algumas redes sociais possuem aplicativos que divulgam sua localização publicamente, mas geralmente você pode desativá-lo nas configurações.
3. Alguns aplicativos esportivos possuem um modo “privado” para que você ainda possa acompanhar suas rotas e competir com amigos, mas apenas com aqueles que você escolher.
4. Esteja atento ao compartilhar sua localização. Somente a envie para a pessoa ou grupo de pessoas que deve recebê-la.
5. Geralmente, você pode definir um período de tempo para o compartilhamento da sua localização – uma hora, o dia todo, para sempre. Escolha a menor unidade de tempo possível caso você esqueça de desligá-lo.

Global Encryption Coalition

Tradução por

Instituto de Pesquisa em Direito & Tecnologia do Recife

PAIS E MÃES

Aplicativos de mensagens instantâneas

Quem realmente está no seu chat em grupo?

As mensagens instantâneas são essenciais para muitas famílias. Aprenda como manter suas questões familiares longe de curiosos e invasores.

A gente está tão acostumado com mensagens instantâneas que se tornou natural compartilhar um link, uma foto, um comentário ou uma gravação de voz – todos mundo tem aquele amigo que só manda áudio – em uma conversa.

Muitos de nós usamos serviços de mensagens instantâneas para manter contato com amigos e entes queridos ao redor do mundo. Usamos esses serviços para planejar encontros, festas, reuniões e casamentos, e pedir pizza, táxis ou compras do dia-a-dia.

Porém, mesmo que você não esteja ouvindo todos esses áudios, outra pessoa pode estar.

Várias pessoas estão digitando... mas quem está lendo?
As mensagens instantâneas originalmente faziam parte de salas de bate-papo e serviços semelhantes e funcionavam apenas em computadores. Mesmo os primeiros serviços de redes sociais ofereciam apenas uma caixa de mensagens.

Agora as mensagens instantâneas estão incorporadas em telefones, jogos, redes sociais e até mesmo em serviços de streaming. Você pode pedir comida, olhar sua conta e até mesmo fazer terapia por meio de aplicativos de mensagens.

Nossos dias estão cheios de barulhos e vibrações de notificações em nossos dispositivos, trazendo atualizações e demandas de casa, da escola, de amigos e de trabalho. Mas quão privadas são suas mensagens privadas?

Imagine que alguém pudesse ver a conversa do seu grupo de família. Seria possível saber que seu amigo de Alagoas vai se casar e que seu amigo de Brasília está se divorciando. Seria possível identificar sua casa pelas fotos, saber os nomes dos seus animais de estimação, o que seus filhos gostam na pizza e que seu adolescente precisa ser lembrado constantemente de que está frio - cadê seu agasalho?

Imagine como seria fácil para alguém usar essas informações para convencer seu filho de que ele é um amigo da família ou um primo esquecido, e o perigo que isso poderia representar. Mas calma, não exclua todos os seus aplicativos de mensagens ainda. Esse chat em grupo tem o registro de tanta coisa de sua família e é possível mantê-lo mais seguro.

Em serviços que não são seguros, como aqueles que não criptografam suas informações, suas mensagens podem ser acessadas. Pode ser para criar um perfil para que você seja alvo de anúncios. Em outros casos, essa conexão insegura pode ser usada por invasores. Eles podem monitorar suas conversas e obter informações sobre seus filhos.

Calma: veja por que você não precisa entrar em pânico

É fácil presumir que todos os serviços de mensagens instantâneas são iguais, mas alguns são realmente mais seguros que outros. Você pode escolher aqueles que oferecem criptografia de ponta-a-ponta, o que significa que suas fotos, vídeos e conversas permanecem privadas. Aquela gravação de voz que você nunca vai ouvir? Ninguém mais vai conseguir ouvir também. Nem mesmo a empresa que presta o serviço de mensageria.

Criptografia significa que seu amigo no Rio de Janeiro pode inundar você com mensagens sobre os planos de casamento, e seu amigo pode despejar os traumas do divórcio dele lá de Brasília, e apenas aquela pessoa curiosa atrás de você no ônibus pode vê-lo (mas você também pode conseguir um protetor de tela contra isso).

O que recomendamos

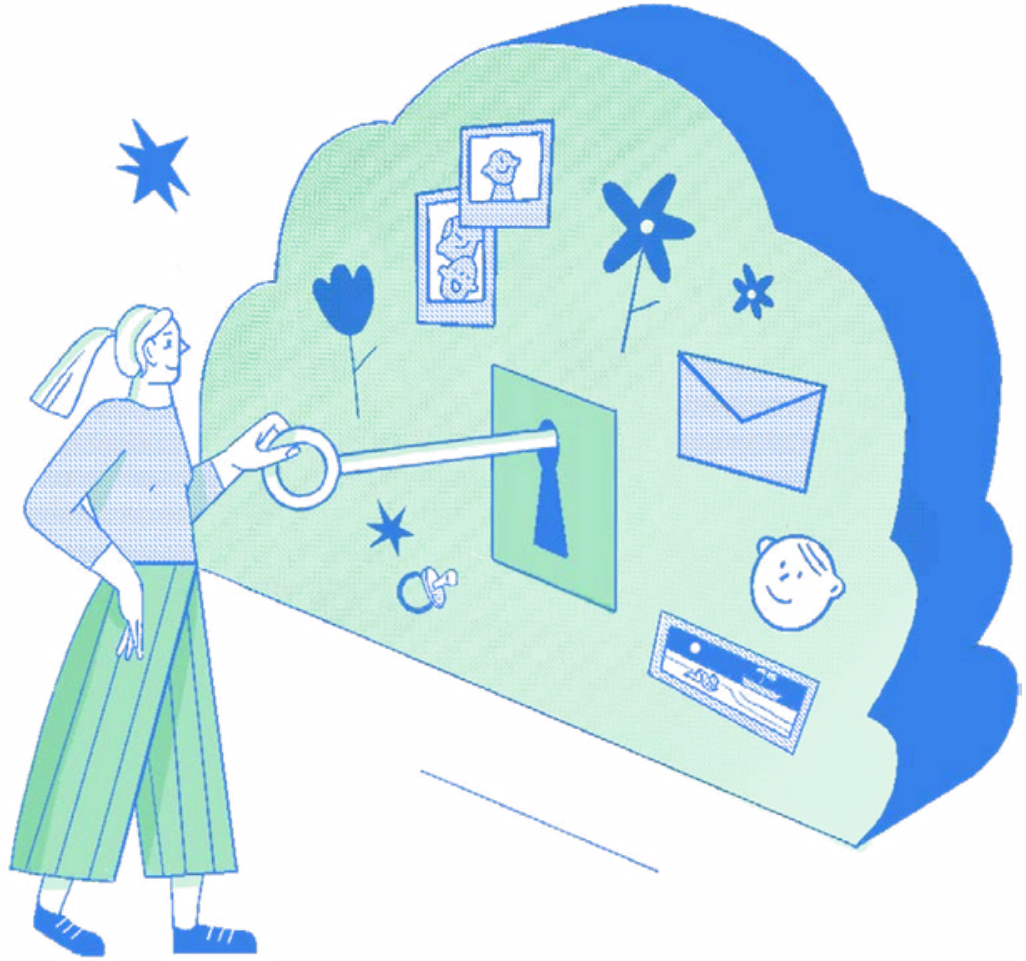
1. Descubra se os serviços de mensagens instantâneas que sua família usa oferecem criptografia de ponta-a-ponta. Se não estiver ativada por padrão, certifique-se de ativá-la.

2. Escolha serviços de mensagens criptografadas, para que você possa conversar em segurança com todos, até mesmo com aquele amigo que só manda gravação de voz.

PAIS E MÃES

Armazenamento em nuvem

Quem está com a cabeça (e olhos)nas sua nuvem?



Armazenar dados na nuvem significa que você pode manter todas as memórias preciosas. Descubra como manter essas fotos e vídeos mais seguros.

Você provavelmente tem milhares (ou dezenas de milhares) de fotos e vídeos de crianças, animais de estimação e familiares. Tiramos fotos de refeições memoráveis, decoração de casa e ocasiões sociais.

E agora, graças ao armazenamento em nuvem, você pode manter todos os vídeos dos seus filhos no Carnaval e todas as fotos do seu cachorro fofinho.

Alguém está mantendo esse espaço de armazenamento protegido de olhares indiscretos – ou algo ainda pior?

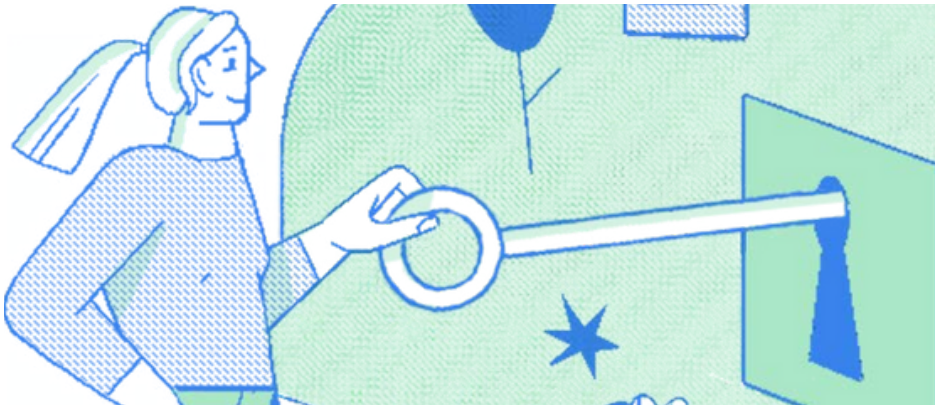
A nuvem é (tipo) o computador de outra pessoa

As câmeras em nossos dispositivos móveis evoluíram tanto que muitas vezes são melhores do que qualquer câmera que já tivemos antes. A qualidade da câmera é uma chance para transformarmos ainda mais momentos em memórias de alta definição. Todas essas fotos precisam ser armazenadas em algum lugar, e muitos de nós fazemos backup no armazenamento em nuvem, às vezes até diariamente.

Talvez você já tenha ouvido: “A nuvem é o computador de outra pessoa”. Apesar de ser uma grande simplificação, seus dados realmente estão armazenados em outro lugar, usando software e hardware controlados por alguém que você nem conhece. Essa é uma boa oportunidade para a gente parar e se perguntar em quem confiaríamos nossas imagens de ultrassonografias, vídeos de nascimento, o primeiro bolo de aniversário esmagado pelo bebê ou a foto do seu cachorro absurdamente fofinho.

Se você não estiver usando um serviço criptografado para armazenamento em nuvem, pessoas mal-intencionadas poderão acessar essas imagens. Claro que mais pessoas deveriam ver como seu cachorro é fofo, mas você não quer que nenhuma de suas fotos ou vídeos sejam compartilhados com alguém além daqueles grupos que você escolheu.

E com certeza você não quer que as fotos de seus filhos caiam nas mãos de pessoas realmente maliciosas. Essas fotos poderiam ser usadas para criar outras imagens, treinar modelos de IA para propósitos com os quais você não concorda ou compartilhadas para fins muito piores.



Calma: veja por que você não precisa entrar em pânico
Você não precisa de mais preocupação com a segurança de seus filhos, então fique tranquilo. Tudo isso pode ser facilmente evitado. Seu serviço de armazenamento em nuvem pode até já estar usando criptografia.

Se ele protege os dados armazenados (ou seja, os dados que estão “em repouso” nesses discos rígidos online), não importa se outras medidas de segurança falharem e alguém baixar o conteúdo. As fotos do seu cachorro, os vídeos do Carnaval e as fotos “antes” da reforma da sua casa seriam apenas um monte de letras embaralhadas. Atores maliciosos não seriam capazes de usar seus arquivos para nada.

O que recomendamos
1. Verifique as configurações e recursos do seu armazenamento em nuvem. Se o serviço oferecer criptografia, mas não estiver ativo por padrão, basta ativar.

2. Se você ainda não escolheu um serviço, reserve um tempo para encontrar o serviço certo – as informações deste guia podem ajudar.

3. Se descobrir que seu serviço de nuvem não oferece criptografia, considere mudar para um que ofereça. Sim, vai ser doloroso mover suas coisas, mas você estará de verdade muito mais seguro.

4. Ao compartilhar links para imagens ou arquivos, verifique as configurações para que o compartilhamento seja apenas com o destinatário pretendido e apenas o conteúdo que você escolheu possa ser visto.

CRIANÇAS E ADOLESCENTES

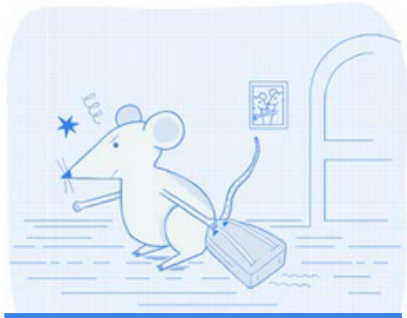
Falando com suas crianças sobre criptografia

Você já conversa com seus filhos sobre segurança e privacidade. Então você sabe que é vital fazer isso de uma forma que os ajude a compreender a urgência, sem assustá-los ou fazê-los sentir que não podem fazer nada divertido. Nossas histórias em quadrinhos podem te ajudar a iniciar essa conversa.

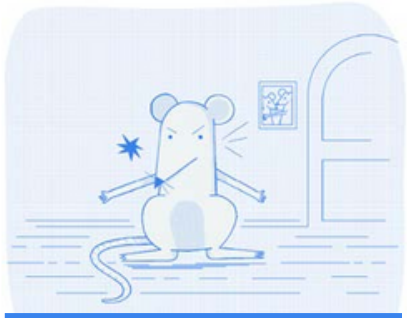
CRIANÇAS E ADOLESCENTES

Cadê a privacidade de Luizinho?

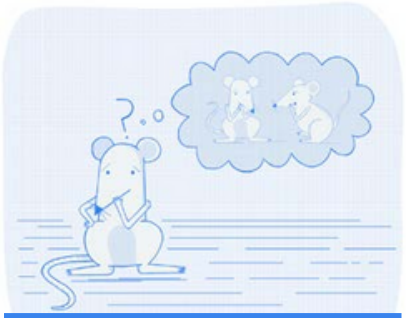
Quando Luizinho chega da escola, geralmente está de bom humor. Hoje não.



E aí, Luizinho?



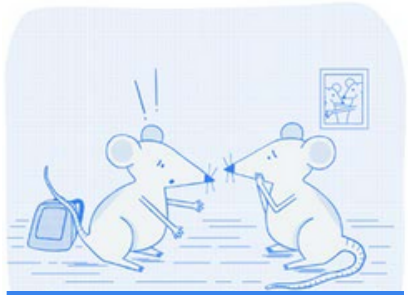
Você contou a sua melhor amiga seu maior segredo e ela contou a todo mundo? Como você se sente agora?



Você conversou com sua amiga sobre como isso fez você se sentir? Não?

Talvez seja uma boa ideia. Afinal, ela é sua melhor amiga há muito tempo...

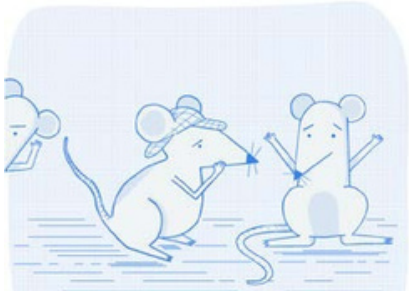
No dia seguinte, na escola, Luizinho diz a Laura que não está feliz com o que aconteceu.



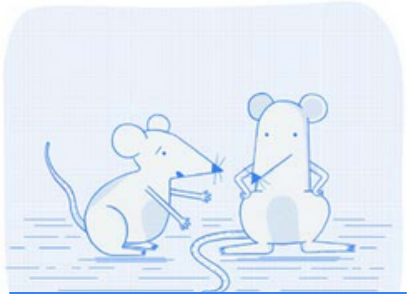
Mas Laura promete que não contou a ninguém.

O mistério é — quem contou o segredo de Luizinho?

Luizinho pergunta por aí...



"Eu ouvi isso de Pedro!" diz Bela. "Pedro ouviu sua conversa com Laura."

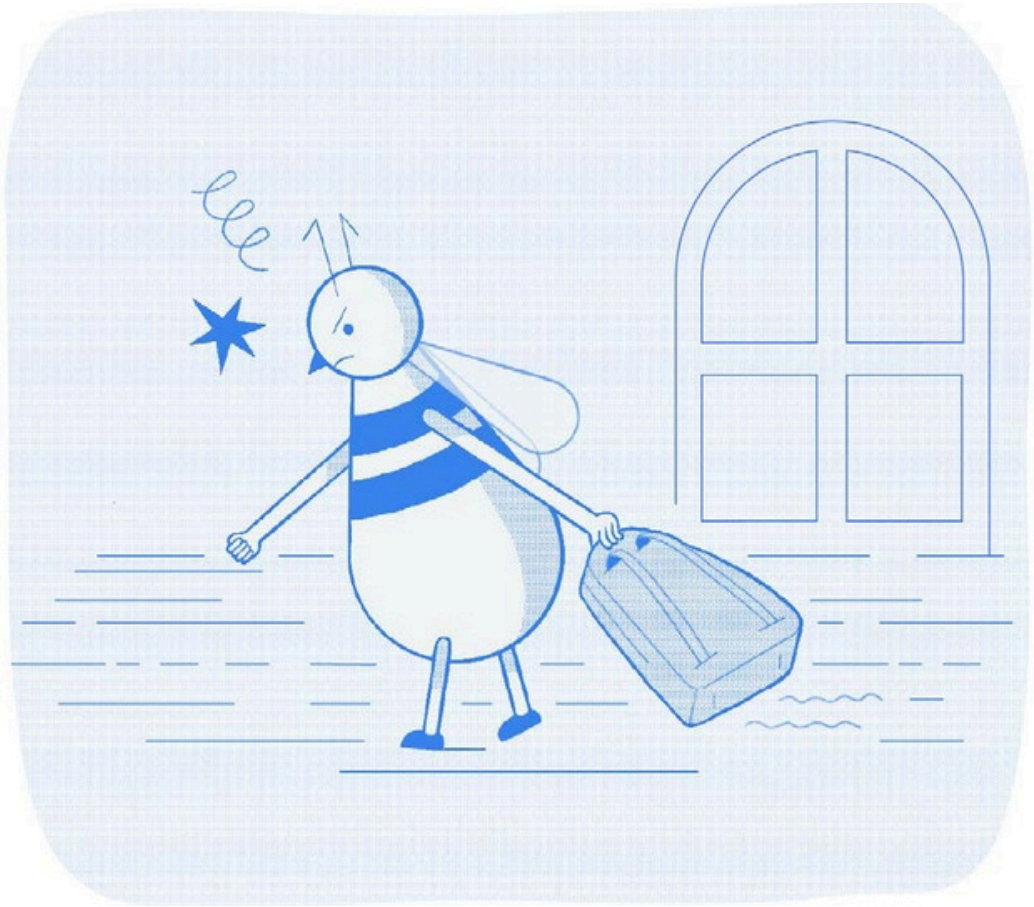


"Sinto muito, Laura", diz Luizinho, "eu deveria ter confiado em você - sei que você é minha melhor amiga".

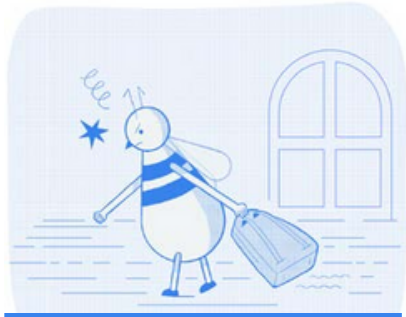
"Não gosto que os outros ouçam nossas conversas. Aqui está um código que podemos usar para mensagens privadas."

CRIANÇAS E ADOLESCENTES

Cadê a privacidade de Joana?

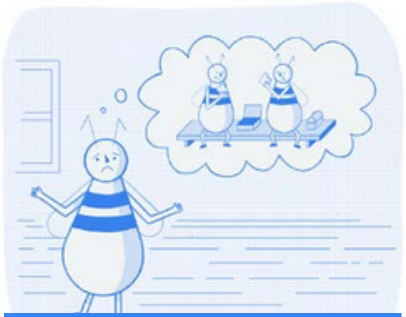


Ei, Joana, tudo bem? Você não parece alegre como sempre.



"As pessoas diziam coisas estúpidas na escola."

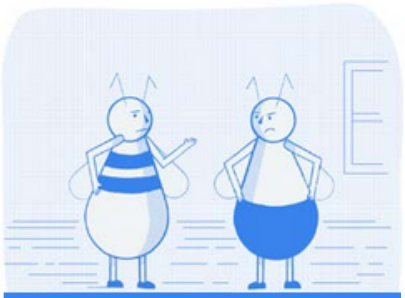
"Eles estavam inventando coisas sobre mim e minha amiga Débora."



"Débora e eu combinamos de ir ao parque no fim de semana e fazer um piquenique. Ela é minha melhor amiga."

"Mas os outros descobriram e estavam cantando aquela música idiota sobre 'com quem será'. Fiquei com muita vergonha."

No dia seguinte, Joana fala com as crianças que estavam brincando com ela.



"Você não devia escutar minha conversa com Débora. Era privada. E você não devia inventar coisas que não sejam verdade."

Joana e Débora concordam em usar um código secreto para manter suas conversas privadas.

ATIVIDADE FAMILIAR

Faça uma auditoria de criptografia

Muitas empresas que fabricam dispositivos e serviços se esforçaram muito para tornar a segurança e a criptografia fáceis de usar. Porém é importante garantir que ela esteja ativada e que os dispositivos sejam atualizados. Uma maneira inteligente de controlar tudo é reunir a família e realizar uma auditoria de criptografia em casa.

Você precisará de 2 a 3 horas no total, então divida as missões pela capacidade de atenção da família.

Missão 1

Criptografando dispositivos inteligentes

Ache todas os dispositivos inteligentes/conectados

Você provavelmente tem mais dispositivos inteligentes/conectados do que imagina, mesmo que não seja o tipo de família que recebe e-mails na geladeira.

O primeiro passo é encontrar todos eles. Divida sua casa em zonas e mande todos procurarem qualquer coisa que pareça estar conectada à Internet. Se algo for grande demais para carregar, tire uma foto da marca e do modelo. Se você tem filhos pequenos, peça-lhes que tragam brinquedos e dispositivos que emitam sons ou se movam. Vocês podem olhar juntos para ver quais são inteligentes/conectados.

Crie um catálogo

Faça uma lista de tudo que se conecta à Internet. Inclua nomes, tipos de dispositivos e modelo.

Em seguida, acesse a Internet e encontre os manuais do usuário para descobrir quais especificações eles usam. Além disso, veja se há uma central de ajuda para o dispositivo. Ali, você vai conseguir descobrir se eles usam criptografia.

Estejam ou não usando criptografia, a primeira coisa que você deve perguntar é: precisamos que este dispositivo esteja conectado à Internet? Algumas dessas coisas oferecem muitas funcionalidades no modo offline. Talvez você queira se conectar à Internet somente quando precisar atualizar o *firmware** ou outras configurações.

* Firmware é o software de nível mais básico de um dispositivo. Ele dá as ordens diretas para a parte física de um computador, por exemplo.

Para dispositivos criptografados:

- Que tipo de criptografia ele usa?
- Seu firmware está atualizado?
- Você já trocou a senha padrão?

Para dispositivos que não são criptografados:

- Existe algum tipo de criptografia que podemos ativar para isso?
- Podemos substituir este dispositivo por um que ofereça criptografia?

Missão 2

Encontre os Mensageiros

Identifique os canais

Existem serviços de mensagens integrados em mais dispositivos e serviços do que você imagina. Alguns são até essenciais – imagine jogar Among Us sem conversar – mas outros são menos úteis ou podem até representar um risco.

Cada membro da família listará seus aplicativos, jogos, plataformas e outros serviços. Crianças menores podem estar usando jogos sobre os quais você não sabe muito. Eles podem ter trocas de mensagem ou caixas de entrada que você não conhecia, então peça que adicionem os deles também.

Faça sua lista

Peça que todos anotem tudo que usa um serviço de mensagens e anote em quais dispositivos estão ligados.

Para cada um, liste se usam ou não criptografia. Se for oferecido, mas não estiver ativado por padrão, deverá ser possível ativá-lo. Se não tiver certeza, encontre informações on-line, na central de ajuda da empresa ou em fóruns de usuários.

A cada serviço, comece com a pergunta: eu realmente preciso usar isso? Posso conversar com essas mesmas pessoas em outra plataforma?

Alguns serviços de mensagens são perfeitamente seguros, mas mais canais para conversar com outras pessoas significam mais pontos potenciais de entrada para pessoas mal-intencionadas, mesmo que o serviço seja criptografado.

Para serviços de mensagens criptografadas:

- Você sabe que tipo de criptografia ele usa?
- Você está usando a versão mais recente do aplicativo?
- Você precisa usar este serviço?

Para serviços de mensagens que não são criptografados:

- É possível ativar algum tipo de criptografia?
- O recurso de mensagens neste serviço é essencial?
- Você pode conversar com essas mesmas pessoas usando um serviço criptografado?

Missão 3

Atualizar e excluir

Organize seus aplicativos

Todos pegam seus dispositivos móveis – telefones, tablets, relógios, consoles de jogos portáteis – e acessam todos os aplicativos.

Comece suas atualizações

Vá na Play ou App Store e baixe todas as atualizações oferecidas. Se você precisa atualizar o sistema operacional, faça isso também. Essas atualizações geralmente incluem recursos de segurança essenciais, correções e atualizações.

Enquanto está fazendo isso, pare e pense nos aplicativos que você não está usando e que não tem intenção de usar novamente. Além de considerar excluí-los, também considere excluir a conta associada a eles. Não é necessário que uma empresa tenha seus dados, caso ela não necessite.

Para serviços de mensagens criptografadas:

- Você sabe que tipo de criptografia ele usa?
- Você precisa usar este serviço?

Para serviços de mensagens que não são criptografados:

- É possível ativar algum tipo de criptografia?
- Você pode excluir sua conta de usuário e o aplicativo?

Missão 4

Cubra seus rastros

Localize os rastreadores

Agora que você organizou suas telas iniciais, faça uma lista de todos os aplicativos restantes. Adicione colunas para quem os está usando e em quais dispositivos. Em seguida, acesse a Internet e use seu mecanismo de pesquisa favorito (com HTTPS!) para descobrir qual desses aplicativos está compartilhando sua localização. Ele está criptografando esses dados? A maioria oferecerá um tutorial ou um guia fácil para desativar isso. Então vai lá e faça isso.

Também é bom acessar as configurações do seu dispositivo e ver o que ele está compartilhando sobre sua localização, talvez sem você saber. Vai ter coisa bem geral, como seu aplicativo de clima, mas vão ter coisas muito mais específicas do que você imagina.

Para serviços criptografados:

- Você pode desativar totalmente o rastreamento de localização?
- Você pode ligá-lo seletivamente?

Se os serviços de não estiverem criptografados:

- Eu posso ativar e desativar o rastreamento?
- Eu posso substituir este aplicativo por um que seja criptografado?
- Se eu não conseguir limitar o rastreamento de localização, posso baixá-lo novamente quando precisar usá-lo?

Aproveite seu novo nível de proteção

Você terminou!

É hora de relaxar (um pouco). Afinal, a criptografia não é perfeita. Adolescentes e crianças ainda vão nos manter acordados à noite de preocupação. As músicas do Mundo Bita viverão na sua cabeça para sempre. E aquele amigo vai continuar deixando áudios.

É bom fazer uma auditoria como essa a cada poucos meses, mas mesmo uma vez por ano já faz uma grande diferença. Com o tempo, toda a sua família vai desenvolver hábitos melhores: escolher serviços criptografados, ajustar o rastreamento de localização e manter aplicativos e dispositivos atualizados. Até as crianças podem aprender a fazer isso. Elas podem até compartilhar essas novas habilidades com amigos e a escola.

Você também pode contar para seus amigos. Compartilhe este guia nas redes sociais, coloque-o em seu bate-papo em grupo ou inicie uma campanha local com nosso kit de ferramentas de campanha pronto para uso.

Obtenha o kit de ferramentas da campanha

Leitura e recursos recomendados

Mantenha seus dados seguros com um plano personalizado

Histórico de localização: atualização do Android e como proteger seus dados

Considerações sobre dados de localização, privacidade e consentimento explícito

Faça escolhas inteligentes para proteger sua privacidade. Pesquise produtos. Leia avaliações de especialistas. Receba dicas e truques.

Privacidade e proteção: uma abordagem dos direitos das crianças à criptografia

Proteção à privacidade e desenvolvimento da autodeterminação informacional das crianças no Brasil

Por que a criptografia é importante para a privacidade?

Discutir criptografia e a proteção de crianças e adolescentes é urgente

Como configurar o celular para uma criança

Por que pensar em regras para moderação de conteúdo em plataformas digitais?

Razões para pensar duas vezes antes de compartilhar sua localização

Global Encryption Coalition

A Coalizão Global pela Criptografia promove e defende a criptografia em países e fóruns multilaterais chave onde ela esteja ameaçada. A Coalizão também apoia os esforços de empresas em oferecer serviços encriptados para seus usuários.

Tradução por

Instituto de Pesquisa em Direito & Tecnologia do Recife

O Instituto de Pesquisa em Direito e Tecnologia do Recife é um centro independente com atuação em pesquisa científica, incidência, capacitação e comunicação focado nos impactos sociais, éticos e jurídicos do desenvolvimento tecnológico.