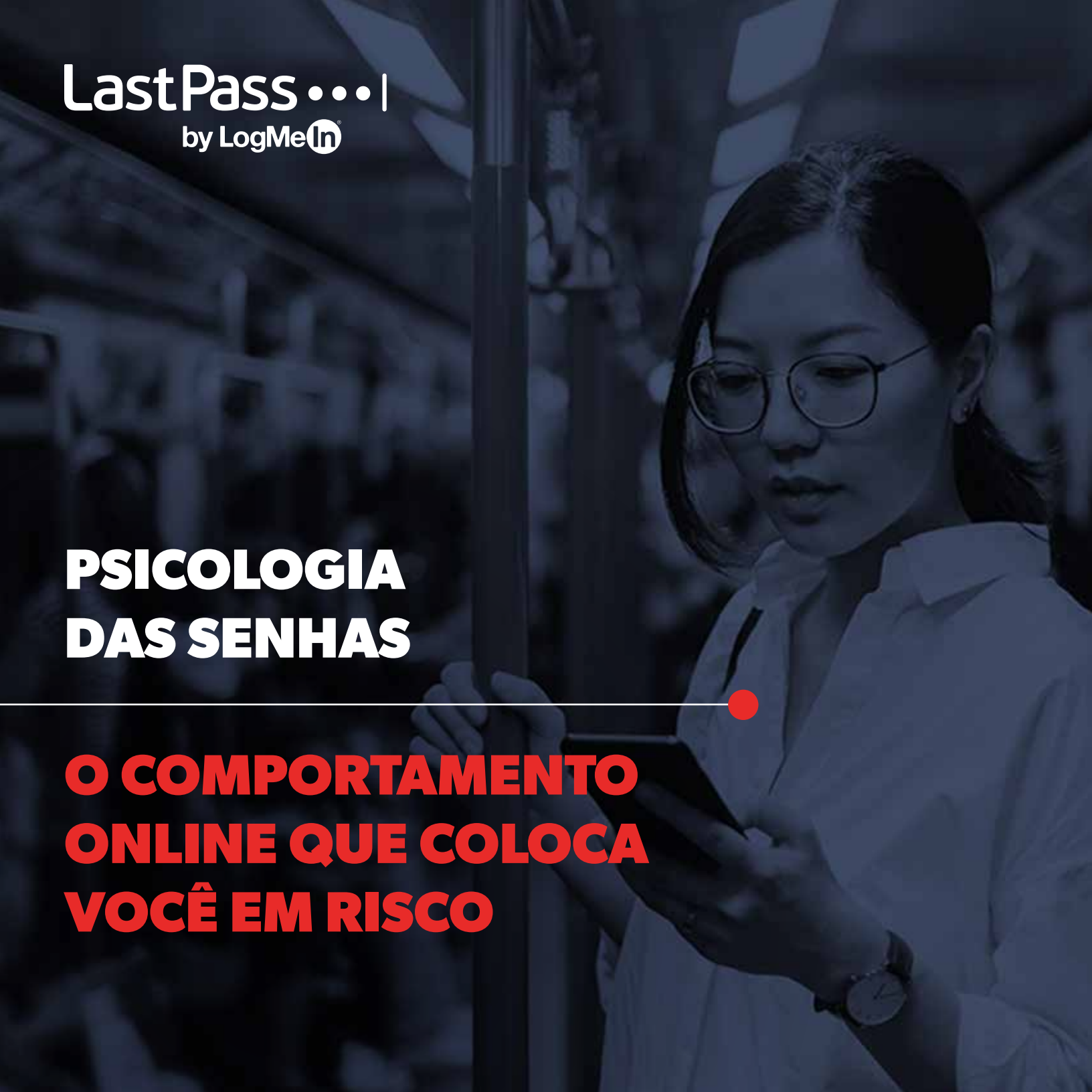
LastPass •••|
by LogMeIn

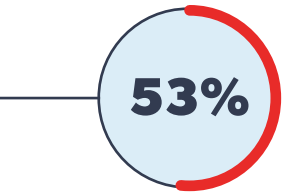


PSICOLOGIA DAS SENHAS

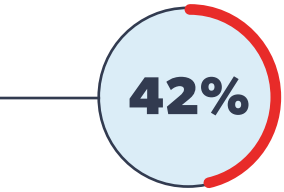
O COMPORTAMENTO ONLINE QUE COLOCA VOCÊ EM RISCO

A DISSONÂNCIA COGNITIVA PREVALECE – SERÁ QUE 2020 É O ANO DA VIRADA PARA O COMPORTAMENTO ONLINE?

Nossa pesquisa Psicologia das Senhas examinou o comportamento online de 3.250 pessoas e mostra que elas não estão se protegendo contra os riscos de segurança digital, mesmo sabendo que deveriam mudar essa postura. A dissonância cognitiva prevalece.



não alteraram suas senhas nos últimos 12 meses, mesmo após ouvirem falar de casos de vazamento de dados nas notícias.



afirmam que ter uma senha fácil de lembrar é mais importante do que ter uma senha segura.

Com cada vez mais pessoas trabalhando e socializando online, é mais importante do que nunca proteger a sua identidade digital. Infelizmente, percebemos um salto nas tentativas de invasão, incluindo malwares de downloads de softwares não verificados e um aumento nos ataques de phishing.

Será que esse é o ponto de partida para as pessoas se preocuparem mais com seus dados online?

Os dados dessa pesquisa servem de referência para mostrar a situação atual do comportamento online dos usuários e explorarão os pontos positivos e negativos deles. Continue a leitura para conhecer os hábitos de pessoas como você e não cometa os mesmos erros.

QUASE TODO MUNDO SABE O QUE É CERTO, MAS, MESMO ASSIM, AGE ERRADO

Nossa pesquisa mostra que a maioria das pessoas acredita conhecer os riscos da segurança precária das senhas. No entanto, elas não aplicam esse conhecimento para se proteger das ameaças digitais.

O que as pessoas falam

91%

91% afirmam saber que usar a mesma senha ou variações de uma senha pode ser arriscado...

80%

80% concordam que o comprometimento de suas senhas é algo preocupante...

77%

77% afirmam estar informadas sobre práticas recomendadas de proteção de senha...

O que as pessoas fazem

66%

... mesmo assim, ao criar senhas, 66% dos participantes sempre ou quase sempre usam a mesma senha ou variações de uma senha – revelando um aumento de 8% em comparação aos dados de 2018.

48%

... mesmo assim, 48% afirmam que, se não houver uma obrigação, nunca alteram suas senhas – revelando um aumento de 40% em comparação aos dados de 2018.

54%

... mas 54% decoram as senhas para controlá-las

NÃO SUBESTIME SEU RISCO

Embora as contradições reveladas pela nossa pesquisa sejam preocupantes, elas nos mostram que as pessoas pensam na segurança das senhas e se consideram bem informadas. Então, por que não estão usando esse conhecimento para se proteger?

Parte do problema é o fato de subestimarem o risco.

Muitos não percebem o quanto de suas vidas estão online. Quando perguntamos quantas contas online os participantes tinham, **71% responderam de 1 a 20**. No entanto, segundo dados anonimizados de usuários do LastPass, **a média aproximada desse número entre pessoas físicas chega a 38 contas online –** quase o dobro do que os participantes da pesquisa acreditam ter.

Por que é importante saber disso?

Cada conta online é um ponto de vulnerabilidade a ser explorado, e as pessoas não percebem quantas portas de entrada os hackers têm para invadir suas vidas. Esse número de contas online só vai aumentar com a vida social e profissional de todos acontecendo normalmente na Internet.

Quantas contas online as pessoas acham que têm

1-20

Quantas contas online as pessoas têm em média

≈ 38

Todo mundo é um alvo

As pessoas também subestimam o valor de seus dados.

42% dos participantes da pesquisa consideram que suas contas não são valiosas o suficiente para compensar o tempo de um hacker.

Os hackers invadem sites com grandes fluxos de acesso para roubar bancos de dados inteiros.

Embora o número do seu cartão de crédito possa valer apenas **US$ 5 para um hacker na dark web**[1], se ele roubar centenas de milhares de dados em uma tacada só, esse valor fica astronômico. Depois, basta que esse hacker use os dados roubados para ter acesso a sites mais importantes, como sites de bancos e serviços financeiros. **Não baixe a guarda.**

Quantas pessoas consideram que suas contas não compensam o tempo de um hacker

42%

SUA NECESSIDADE DE CONTROLE ESTÁ COLOCANDO VOCÊ EM RISCO

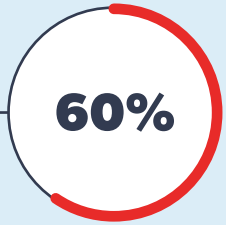
A reutilização de senhas é o maior erro de segurança que os participantes da nossa pesquisa cometem. Quando perguntamos com que frequência eles usam a mesma senha ou uma variação de uma senha, **66% responderam que sempre ou quase sempre** – revelando um **aumento de 8% em comparação aos dados de 2018.**

Nada mudou desde 2018?

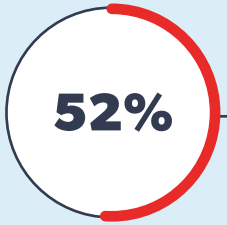
A dissonância cognitiva continua sendo a tendência por aqui. Os participantes da pesquisa têm consciência do que deveriam fazer, mas não agem de acordo com esse conhecimento. **Por quê?**

As pessoas parecem ignorar os riscos que senhas pouco seguras geram. Tecnologias como a biometria estão deixando as senhas textuais cada vez mais em desuso, e muita gente simplesmente se sente confortável em usar o "esqueci minha senha" sempre que não consegue entrar em suas contas.

Quando perguntamos por que os participantes da pesquisa reutilizavam senhas, ouvimos respostas idênticas às de 2018:



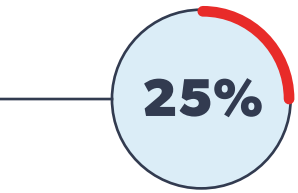
Tenho receio de esquecer meus dados de login



Quero estar no controle e saber todas as minhas senhas

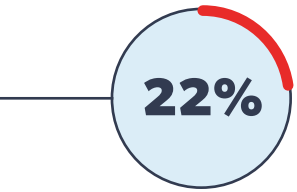
Essa necessidade de controle é compreensível, mas equivocada. Embora haja uma sensação de segurança por saber que todas as suas senhas são iguais, a reutilização delas aumenta muito o seu risco em comparação a quando você cria uma única senha para cada conta.

Além disso, tentar se lembrar de todas as senhas não funciona.



redefinem as senhas uma ou mais vezes por mês porque as esquecem

E, por ter de usar a memória, elas são previsíveis e carecem de segurança:



afirmam ser capazes de adivinhar a senha de seu parceiro

Por que a reutilização de senhas é tão arriscada?

O problema de reutilizar senhas em todas ou na maioria das suas contas é o seguinte: se um hacker tiver acesso a uma conta, ele tem acesso a todas as outras. Além disso, ao reutilizar senhas em contas pessoais e do trabalho, você acaba colocando sua empresa em risco também.

O QUE MAIS VOCÊ PODE FAZER PARA PROTEGER SUAS CONTAS?

Além de criar senhas fortes e únicas – que, diga-se de passagem, é um primeiro passo essencial –, há outras ferramentas para proteger suas contas online.

A autenticação multifator (MFA) é uma camada extra de segurança fácil de adotar. A boa notícia é que há mais conscientização e uso da autenticação multifator. **Apenas 19% dos participantes da pesquisa** afirmaram **não saber o que é autenticação multifator**, enquanto **54% dos participantes** afirmaram usar esse recurso em suas **contas pessoais** e **37% usam nas contas do trabalho**.

Os participantes da pesquisa também se sentem muito confortáveis com a autenticação biométrica, que usa impressões digitais ou reconhecimento facial para efetuar login em dispositivos ou contas. **65% dizem que confiam mais na impressão digital ou no reconhecimento facial** do que nas senhas textuais. O conforto com a biometria provavelmente se deve à frequência de uso dos dispositivos móveis.

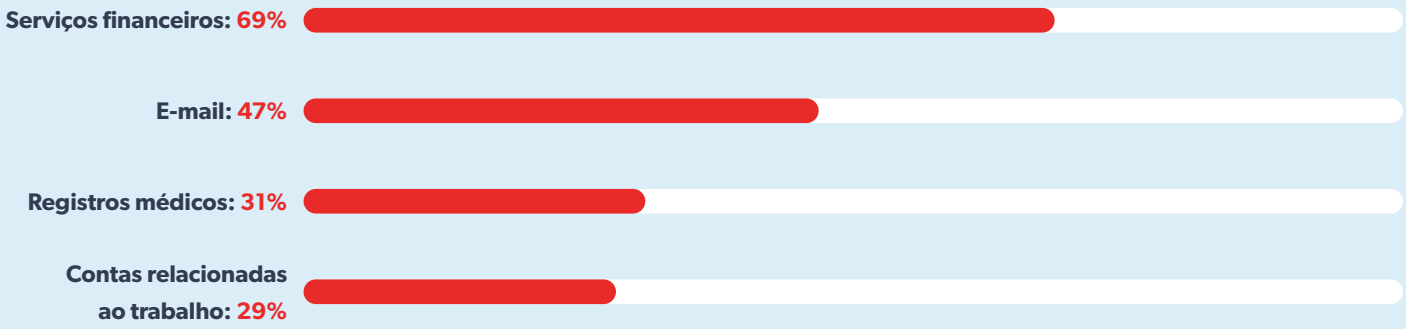
O que é a autenticação multifator?

A autenticação multifator é uma ferramenta que exige mais do que seu nome de usuário e senha para efetuar login em uma conta. Depois de digitar seu nome de usuário e senha, a autenticação multifator solicita uma segunda informação, como um código único ou sua impressão digital.

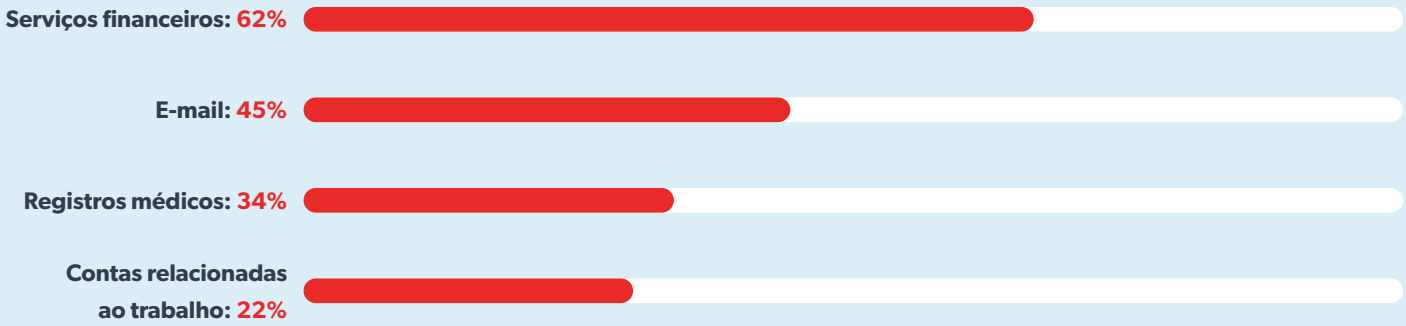
DOIS TIPOS DE CONTA CHAMAM A ATENÇÃO DOS USUÁRIOS: CONTAS DE E-MAIL E DE SERVIÇOS FINANCEIROS

Os participantes da pesquisa reconhecem que contas de e-mail e de serviços financeiros precisam de mais proteção, revelando um instinto de perspicácia. Seu endereço de e-mail é o coração da sua vida online e costuma conter informações que os hackers podem usar para roubar sua identidade e acessar outras contas. Suas contas de serviços financeiros são obviamente essenciais porque dão acesso ao seu dinheiro, informações de crédito e outros dados sensíveis.

Para quais contas você criaria senhas mais seguras?



Em quais contas você habilita a autenticação multifator?



É animador perceber que as pessoas entendem a importância de proteger suas contas de e-mails e serviços financeiros. No entanto, é crucial que todo mundo estenda essas proteções a todas as outras contas.

Atenção, empresas!

Os participantes da pesquisa estão protegendo menos as contas de trabalho do que as contas pessoais. Esses hábitos ruins de segurança afetam os dados pessoais e acabam se estendendo também à sua empresa.

PANORAMA REGIONAL

Até aqui, nosso relatório levou em consideração dados globais, mas será que as tendências são diferentes se considerarmos países específicos?

A Alemanha tem consciência do risco
Embora o GDPR possa dar destaque ao risco de uma proteção precária da privacidade de dados, a legislação não está estimulando os comportamentos ideais.

94% dos participantes da pesquisa sabem do risco de usar senhas parecidas, mas 30% usam uma variação de 1 ou 2 senhas, e mais 30% não estão preocupados com o comprometimento de suas senhas.

O Brasil é promissor
A regulamentação pendente da LGPD aumentará a vigilância online.

94% dos brasileiros se preocupam em ter suas senhas comprometidas, e 64,8% concordam que suas contas têm valor para hackers.

Com 78% confiando mais na biometria do que nas senhas tradicionais, a autenticação multifator pode ser a camada extra de segurança de que os brasileiros precisam.

Singapura é um exemplo a ser seguido
Dada a atenção em se criar e sustentar uma economia digital pulsante, não é de se surpreender que 88% das pessoas saibam que usar a mesma senha ou variações de uma senha seja um risco. Esses dados podem explicar por que:

40% criam uma senha mais segura e mais complexa para as contas do trabalho.

A autenticação multifator é amplamente usada tanto em contas pessoais (70%) quanto em contas do trabalho (58%)!

O Reino Unido é campeão em contas online
Mesmo com o **NCSC** trabalhando na conscientização de boas práticas online, o efeito ainda é pouco, já que 58% dos participantes não alteraram suas senhas mesmo após ouvirem falar de casos de vazamento de dados nas notícias!

92% sabem que usar a mesma senha ou variações de uma senha pode ser arriscado, mas têm esse hábito mesmo assim

64% dos participantes da pesquisa reutilizam senhas por terem receio de esquecê-las.

A Austrália está fazendo o dever de casa, mas ainda há confusão entre os usuários
Com os excelentes relatórios de **NDB**, que detalham vazamentos de dados e suas fontes, é interessante perceber que 80% se consideram bem informados sobre prática recomendadas sobre senhas, no entanto:

Somente 18% criam senhas únicas e complexas para suas contas de trabalho, e para 36% não há diferença entre as senhas pessoais e do trabalho.

E, embora 90% reconheçam o risco, 69% usam sempre ou quase sempre a mesma senha ou variações uma senha.

O comportamento relacionado a senhas dos Estados Unidos deixa a desejar, mas a autenticação multifator é forte

60% dos americanos têm receio de esquecer os dados de login e, para evitar isso, 33% registram suas senhas em algum lugar

67% confiam mais na biometria do que nas senhas textuais tradicionais

42% usam a autenticação multifator nas contas do trabalho e 58% nas contas pessoais, superando todas as outras regiões, atrás apenas de Singapura

PARE DE SE COLOCAR EM RISCO

Você está sempre pensando em se proteger e garantir a segurança da sua família. Talvez você não tenha pensado em estender esses esforços para a vida online, e isso não precisa ser difícil.

Faça com que 2020 seja o ano da virada no seu comportamento online

Deixe que um gerenciador de senhas se lembre das suas senhas e as preencha para você. Nós entendemos a sua vontade de estar no controle, mas é mais seguro criar senhas seguras e únicas para cada conta e armazená-las em um cofre criptografado. Você nunca mais vai se estressar para se lembrar de senhas e vai ter a tranquilidade de saber que estão guardadas em segurança para quando precisar delas.

Use a autenticação multifator. Comece pelas contas essenciais e mais utilizadas, como e-mail, bancos, cartões de crédito, impostos, redes sociais. Depois, a cada conta nova, habilite a autenticação multifator se for uma opção disponível.

Monitore seus dados. Independentemente de você usar serviços de monitoramento de crédito da administradora do seu cartão de crédito ou serviços de monitoramento da dark web, sempre saiba quando seus dados foram comprometidos.

O LastPass já conquistou mais de 17 milhões de usuários e 61 mil empresas para armazenar e preencher senhas, números de cartão de crédito e outros dados pessoais. Use o LastPass para gerar senhas seguras e preenchê-las automaticamente ao visitar sites e aplicativos, em todos os seus dispositivos.

Saiba mais sobre o LastPass para usuários individuais, famílias e empresas de todos os portes em **www.lastpass.com**.

Fontes:
1 https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

04.14.2020/LMI1249/PDF