

LastPass...|

Psicologia das Senhas

Vidas digitais cada vez mais ativas
e (maus) comportamentos de senhas



Segurança de senhas em 2021: superando as vulnerabilidades humanas

A pandemia de covid-19 afetou o local de trabalho de milhões de pessoas no mundo todo. Com escritórios físicos fechados, muitas pessoas passaram a trabalhar em casa. Sem ter para onde ir, a vida online virou rotina.

O risco para indivíduos e empresas nunca foi tão grande.

Hackers estão aproveitando e explorando vulnerabilidades humanas como nunca. Os tipos de ataques mudaram devido ao grande número de pessoas trabalhando remotamente e passando mais tempo online.

De acordo com o Data Breach Investigations Report (DBIR) de 2021, os cibercriminosos estão visando cada vez mais indivíduos e seus dispositivos.

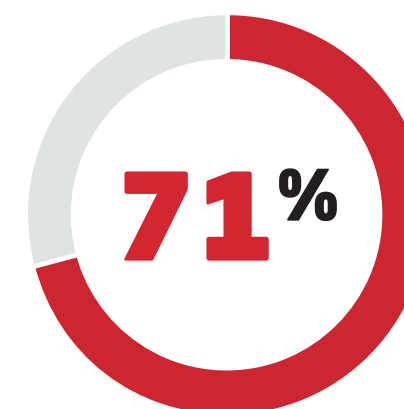
85%

A maioria dos vazamentos de dados — assustadores 85% — envolveu um elemento humano (phishing, credenciais roubadas e erro humano).

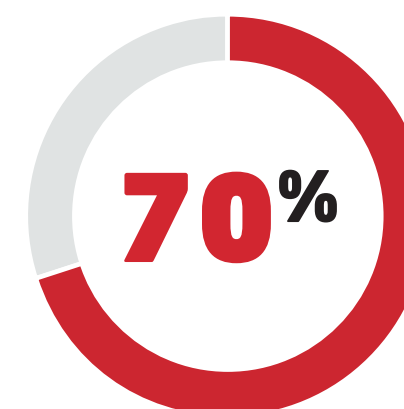
36%

36% dos vazamentos no ano passado envolveram phishing — 11% a mais do que no ano anterior.

Durante a pandemia:



atuaram em um regime total ou parcialmente remoto.



passaram mais tempo online por questões de entretenimento pessoal e trabalho.

Visão geral da pesquisa

Nosso relatório de Psicologia das Senhas explora os comportamentos de segurança de senhas de 3.750 profissionais em sete países. Perguntamos aos participantes sobre seus sentimentos e comportamentos em relação à segurança online.

Países que participaram da pesquisa:

- Estados Unidos
- Austrália
- Reino Unido
- Cingapura
- Alemanha
- Índia
- França

Muita conscientização, pouca ação

O que as pessoas falam.

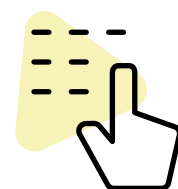
79%

concordam que senhas comprometidas são preocupantes...



92%

sabem que é arriscado usar a mesma senha ou uma variação dela...



O que as pessoas fazem.

51%

... confiam na memória para manter as senhas sob controle.

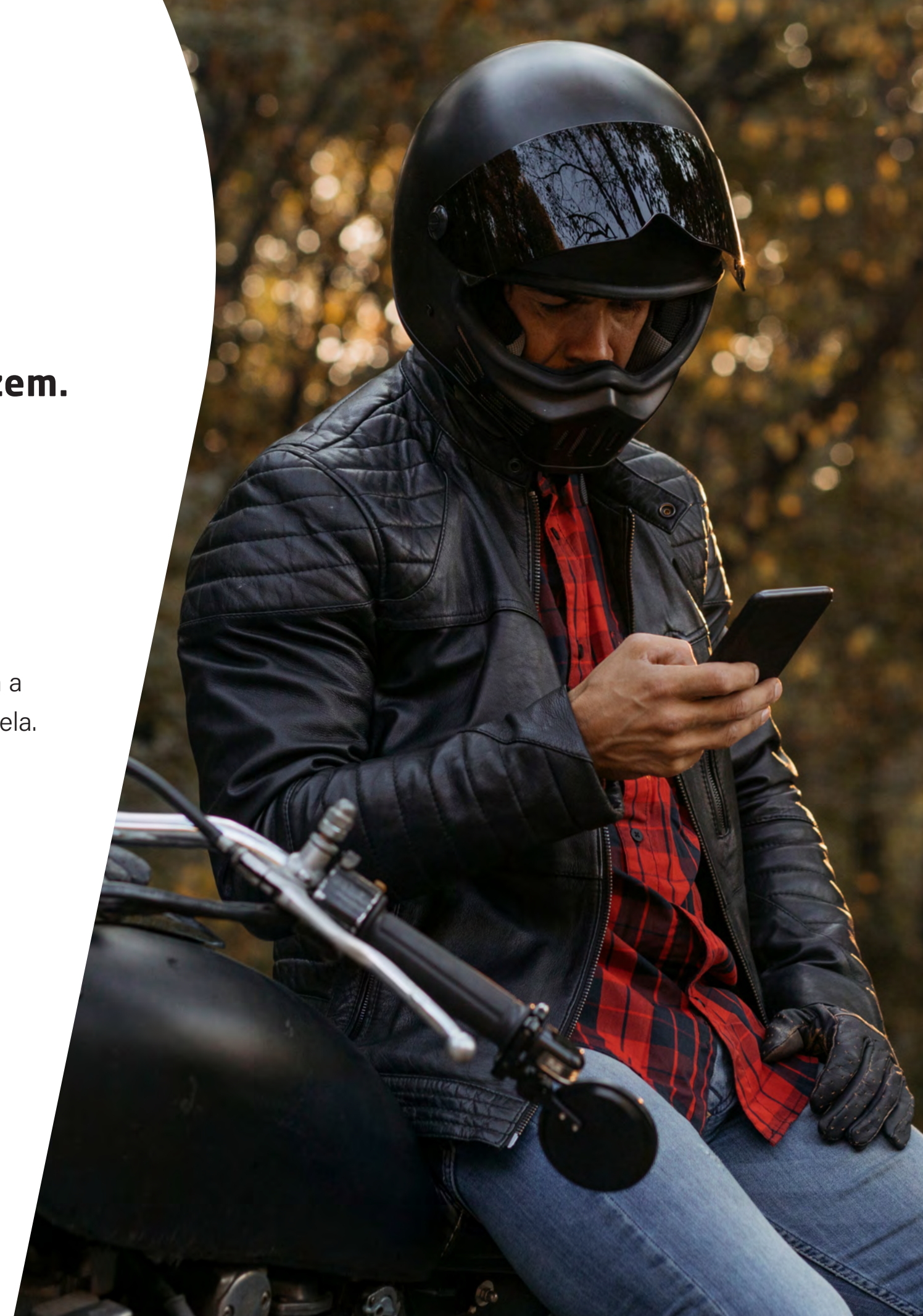
65%

... sempre ou quase sempre usam a mesma senha ou uma variação dela.

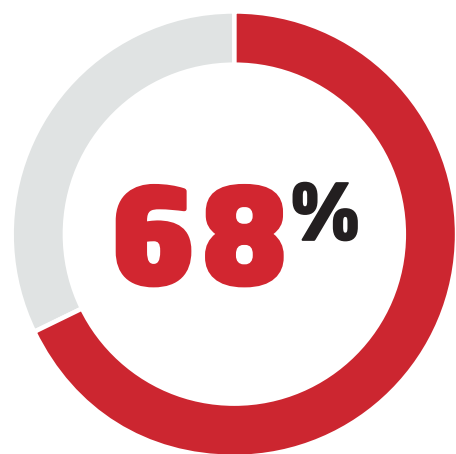


45% NÃO ALTERARAM AS SENHAS

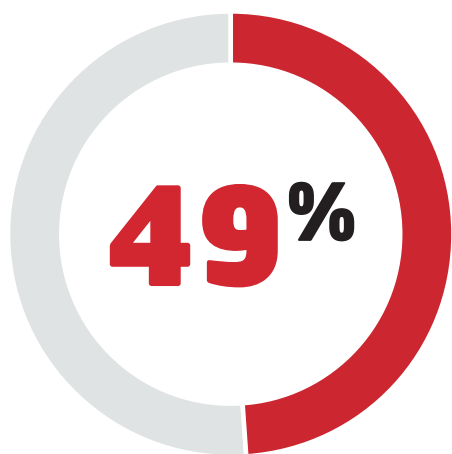
45% dos participantes da pesquisa não alteraram as senhas no ano passado, mesmo após um vazamento.



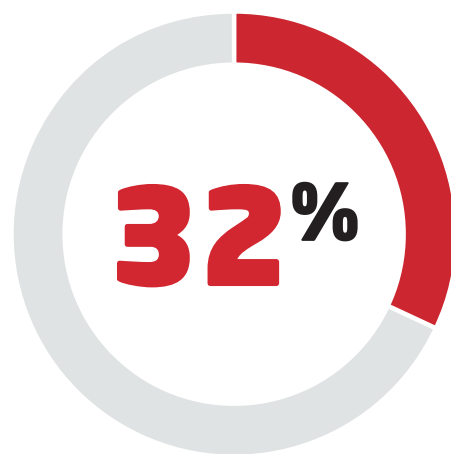
As pessoas praticam uma segurança de senhas seletiva, mas criariam senhas mais seguras para:



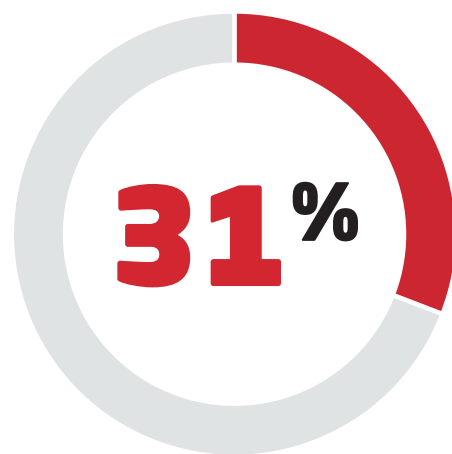
Contas financeiras



Contas de e-mail



Contas relacionadas ao trabalho



Registros médicos

8%

Apenas 8% disseram que uma senha segura não deve estar vinculada a informações pessoais.

Isso significa que a maioria dos usuários está criando senhas que utilizam informações pessoais vinculadas a possíveis dados públicos, como aniversário ou endereço residencial.

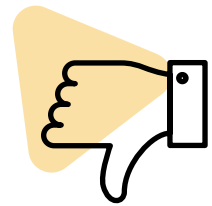


DICA DE OURO

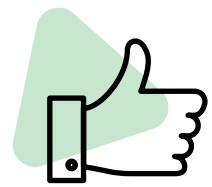
Use frases sem sentido salpicadas de números e símbolos em vez de palavras isoladas para tornar suas senhas mais longas, mais seguras e mais fáceis de lembrar — isso também dificulta a ação de hackers para decifrá-las.

Pontos cegos e pontos de destaque

A dissonância cognitiva prevalece. As pessoas escolhem quais informações elas acham que vale a pena proteger. Como resultado, elas deliberadamente têm comportamentos arriscados relacionados a senhas, mesmo quando passam um tempo online sem precedentes por questões de trabalho e entretenimento durante uma pandemia.



83% não saberiam dizer se suas informações estão na dark web.



76% afirmam usar MFA em contas de trabalho e pessoais, um aumento de 10% em relação ao ano passado.



DICA DE OURO

Trate todas as credenciais como algo vulnerável. Você pode achar que as credenciais da sua academia local não valem nada para os hackers, mas se essas credenciais forem idênticas ou parecidas com o login da sua conta bancária, um vazamento na sua academia pode acabar resultando na exposição de informações financeiras confidenciais.

A expansão da vida digital.

Mais contas do que nunca.



91% dos participantes criaram pelo menos uma nova conta este ano.



90% dos participantes indicam ter até 50 contas online/de aplicativos.

.....

50%

.....

Os participantes têm 50% mais contas em 2021 do que em 2020.



Com nossa presença digital cada vez maior, precisamos de uma proteção mais robusta para nossas informações pessoais.

Nossas vidas digitais passaram por uma expansão significativa durante a pandemia de covid-19.

A desconexão em nossas vidas diárias nos motivou a buscar uma conexão online sem precedentes. O resultado: mais contas criadas, e mais informações pessoais compartilhadas online.



DICA DE OURO

Mantenha suas atualizações nas redes sociais privadas ou faça poucas postagens públicas. Pessoas mal-intencionadas vasculham perfis públicos e podem usar informações aparentemente inofensivas para hackear contas fora das redes sociais.

A quantidade de informações pessoais online está aumentando:

53%

compartilharam fotos de férias.

20%

compartilharam fotos de seus animais de estimação com os nomes deles e, em seguida, usaram tais nomes em senhas, **um aumento de 5% em relação a 2020.**

27%

compartilharam fotos da casa/do bairro onde moram, **um aumento de 7% em relação a 2020.**

Trabalho remoto: perspectivas do funcionário e do empregador

Funcionário hábitos de trabalho remoto:

47% não mudaram os hábitos de segurança online desde que começaram a trabalhar remotamente.

46% não reforçaram as senhas para o trabalho remoto.

44% compartilharam senhas e informações confidenciais de contas profissionais durante o trabalho remoto.

Empregador hábitos de trabalho remoto:

39% tomaram os devidos cuidados para que os funcionários estivessem conectados à rede da empresa por meio de redes seguras durante o trabalho remoto.

35% fizeram com que os funcionários atualizassem as senhas com mais regularidade.

35% aprimoraram os métodos de autenticação.



Os administradores de TI devem estar atentos. A presença de risco não faz com que as pessoas se sintam inerentemente motivadas a adotar uma segurança melhor. Quase metade dos funcionários apresenta comportamentos arriscados relacionados a senhas quando trabalha remotamente.

Os administradores de TI devem repensar as estratégias de segurança da mesma maneira que os funcionários remodelam e reavaliam a forma como trabalham.



DICA DE OURO

Invista em uma solução de **gerenciamento de senhas** para melhorar os hábitos e a segurança relacionados a senhas. Implemente **SSO** e **MFA** para proteger todos os pontos de acesso. Ofereça treinamentos de segurança para instruir e orientar.

Panorama regional:



Reino Unido

61% sabem que uma senha segura e única não está vinculada a informações pessoais.

Eles também foram os menos propensos a compartilhar informações pessoais online **(41%)**.



Alemanha

A Alemanha é líder em conhecimento da dark web **(79%)**.

Apenas **14%** saberiam se suas informações pessoais estivessem na dark web.



França

Apenas **15%** dos participantes franceses trabalharam remotamente durante a pandemia de covid-19.

Apenas **43%** mudaram hábitos de segurança online ao trabalhar remotamente.



Cingapura

Cingapura é o que mais se preocupa com senhas comprometidas **(93%)**.

Eles também estão na liderança no que diz respeito a saber o que fazer caso sejam hackeados **(74%)**.



Índia

A Índia tem uma probabilidade significativamente maior de usar um gerenciador de senhas ou navegador para armazenar senhas do que outros países **(64%)**.

Os participantes indianos foram os líderes em termos de mudança de hábitos de segurança online durante o trabalho remoto **(81%)**.



Austrália

71% dos australianos sempre/quase sempre usam a mesma variação de senha.

No entanto, os australianos passaram menos tempo online, em geral, durante a pandemia **(61%)**.



Estados Unidos

Os americanos estavam mais propensos a usar serviços de monitoramento de crédito se a conta fosse comprometida **(31%)**.

No entanto, **39%** sentiram não haver necessidade de mudar seus hábitos de segurança online ao trabalhar remotamente porque eles já eram seguros.

Ligando os pontos

Por que as pessoas apresentam maus comportamentos relacionados a senhas (quando claramente sabem como devem agir)?

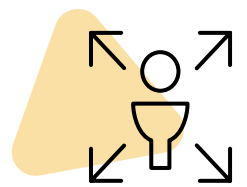
68% dos que reutilizam senhas têm medo de esquecê-las.

52% dos que reutilizam querem estar no controle de todas as senhas.

36% não consideram suas contas valiosas o bastante para hackers.



Por que a reutilização de senhas é tão perigosa, especialmente com a expansão da nossa vida digital?



Uma combinação roubada de nome de usuário e senha dá ao hacker acesso a muitas contas.



Quando um cibercriminoso consegue acessar um dispositivo usado para fins pessoais e de trabalho, ele pode rapidamente obter acesso a uma rede corporativa para roubar dados ou dinheiro.



AS PESSOAS APRESENTAM MAUS COMPORTAMENTOS RELACIONADOS A SENHAS

Com a vida digital em constante expansão e a falta de suporte de segurança cibernética, uma combinação de hábitos, emoções e falta de urgência faz com que as pessoas não mudem seus comportamentos online.

Como combater (maus) comportamentos relacionados a senhas

A pandemia de covid-19 gerou uma mudança sem precedentes na forma como trabalhamos e interagimos. Nós passamos mais tempo online. Compartilhamos mais coisas digitalmente. Se sabemos por que as pessoas estão se comportando dessa maneira, como podemos corrigir esse comportamento?

Como é um bom comportamento relacionado a senhas?

- Torne cada senha única.
- Use combinações de caracteres que não fazem sentido.
- Ative a autenticação de dois fatores.
- Atualize as senhas quando receber uma notificação de vazamento.

▶ Enfrente seu medo.

Use um **gerenciador de senhas** para gerenciar e proteger suas senhas. Deixe um gerenciador de senhas fazer o trabalho de criar, lembrar e preencher suas senhas.

▶ Enfrente sua ansiedade.

Adicione uma camada de segurança com a **autenticação multifator (MFA)** para garantir que você seja a única pessoa com acesso às suas informações.

▶ Enfrente sua apatia.

Monitore seus dados e use o **monitoramento da dark web** para saber se suas informações foram comprometidas.





LastPass...

O LastPass já conquistou mais de 30 milhões de usuários e 85 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**](#)