bet boo - symphonyinn.com

Autor: symphonyinn.com Palavras-chave: bet boo

Notícias Locais: Novo Aplicativo de Senhas da Apple

O assunto quente do dia é a inteligência artificial, ou como alguns podem dizer, a "inteligência Apple". Por isso, acho que é hora de falarmos sobre *sentar de costas na cadeira* senhas.

Embora possa ter sido enterrado na cobertura do evento Apple da noite passada - coberto por nossa equipe **bet boo** Cupertino e Nova York - uma das mudanças mais consequentes que estão por chegar às plataformas da empresa no próximo ano é a criação de um novo aplicativo de Senhas.

Do 9to5Mac:

> O usuário médio provavelmente nunca ouviu falar do 1Password ou do LastPass e pode ou não estar ciente de que o iPhone pode criar e armazenar automaticamente senhas para você. Para usuários como esses, um novo aplicativo de Senhas aparecendo **bet boo bet boo** tela inicial este outono é esperançosamente um passo **bet boo** direção a um futuro de computação mais seguro.

Em suma, é uma mudança mínima. Quase tudo o que o novo aplicativo de senhas fará já está presente no iOS e no macOS, apenas enterrado **bet boo** menus de configurações. A menos que você tenha decidido fazer algo diferente, se você usar qualquer uma das plataformas, deve ser capaz de ir para o aplicativo de configurações do sistema, deslocar-se até Senhas e, após autenticar com **bet boo** face ou impressão digital, ver uma boa lista de todos os logins da internet.

A Apple não negligenciou o serviço. Nos anos desde seu lançamento, ela o desenvolveu **bet boo** um gerenciador de senhas totalmente funcional: ele executa uma leve verificação de segurança, alertando-o sobre senhas hackeadas ou reutilizadas; ele permite que você compartilhe detalhes com membros da família, economizando-o de ter que enviar informações sensíveis por email; ele até permite que você importe e exporte o banco de dados, ainda uma raridade para a empresa.

No entanto, mesmo extrair o serviço para seu próprio aplicativo ainda é um ato importante. Porque o problema que a Apple está tentando resolver não é realmente sobre senhas **bet boo** si - é sobre identidade.

Na semana passada, sentei-me com Steve Won, o diretor de produto-chefe do 1Password, um aplicativo de gerenciamento de senhas com longa tradição nas plataformas da Apple. "A maneira como gerenciamos a identidade digital está completamente enrolada", disse Won. "Efetivamente, eu não tenho uma identidade **bet boo** absoluto: existem apenas bancos de dados aleatórios **bet boo** todo o mundo com minhas informações. Minhas informações de cartão de crédito, informações bancárias, meu universidade provavelmente ainda tem minhas informações, e assim por diante."

As senhas são a forma mais antiga e popular de resolver o problema de identidade na internet. Você prova quem é compartilhando algo que apenas você sabe. Mas elas também têm problemas óbvios e grandes: simplesmente existir no mundo desenvolvido exige a criação de mais senhas do que uma pode razoavelmente se lembrar, o que empurra as pessoas **bet boo** direção à reutilização de senhas. A reutilização de senhas significa que a perda de uma única senha pode levar a hackeamentos subsequentes devastadores. Tentar memorizar uma senha única para cada conta força as senhas a serem curtas o suficiente para serem adivinhadas por força bruta.

Tudo isso leva, inevitavelmente, à criação de gerenciadores de senhas. Apesar de competir diretamente com a Apple neste espaço - uma posição **bet boo** que ninguém escolheria estar - Won é otimista. "Toda vez que a Apple e o Google fazem uma grande empurrada **bet boo** torno

do gerenciador de senhas, é um dos nossos meses de liderança mais fortes", diz. Promovendo o 1Password como "o Aston Martin dos gerenciadores de senhas", ele argumenta que qualquer coisa que deixe claro para os usuários que precisam se afastar da memorização ou reutilização de senhas é um plus. "O mercado alvo total de um gerenciador de senhas deveria realmente ser sete bilhões e meio de pessoas."

Mas mesmo um gerenciador de senhas não pode consertar senhas. Vincular sistemas cada vez mais preciosos a uma cadeia facilmente phishada ou roubada de caracteres é uma receita para problemas. A autenticação de dois fatores resolve algumas das questões, mas também introduz novas. E, portanto, a indústria começou a olhar para o que vem a seguir: chaves de acesso.

De gerenciadores de senha a chaves de acesso, nada parece ter resolvido a crise de identidade da tecnologia até agora.numéro whatsapp 1xbet sénégal

Você se lembra quando falamos sobre eles há dois anos? Do TechScape:

> Uma melhora leve **bet boo bet boo** vida diária. Isso é o que Apple, Google e Microsoft estão oferecendo, com um anúncio raro de que os três gigantes da tecnologia estão adotando o padrão Fido e trazendo um futuro sem senha. O padrão substitui nomes de usuário e senhas por 'chaves de acesso', informações de login armazenadas diretamente **bet boo** seu dispositivo e apenas carregadas para o site quando combinadas com autenticação biométrica como selfies ou impressões digitais.

Desde o lançamento deles **bet boo** 2024, no entanto, as chaves de acesso não pegaram fogo. Parte disso se deve ao fato de **bet boo** implantação ter sido lenta - apenas alguns sites as suportam, com o 1Password listando 168 **bet boo** seu diretório - mas também porque os primeiros usuários foram queimados. O hacker australiano William Brown é representativo dessa reação:

> Around 11pm last night my partner tried to change our lounge room lights with our home light control system. When she tried to login, her account couldn't be accessed. Her Apple Keychain had deleted the Passkey she was using on that site ... Just like adblockers, I predict that Passkeys will only be used by a small subset of the technical population, and consumers will generally reject them.

As próprias coisas que tornam as senhas inseguras - o fato de que elas são legíveis por humanos, que você pode copiá-las e colá-las **bet boo** texto simples, que você pode falar delas ao telefone - também as fazem parecer controláveis. As chaves de acesso exigem que você confie inteiramente no sistema, e após os últimos anos, você pode não ter muita confiança restante.

Para o Won da 1Password, no entanto, a troca ainda é uma oportunidade. "A Apple, a Microsoft e a Google têm sido muito, muito abertas a fazer desta uma discussão conosco, porque elas percebem que as chaves de acesso só vão funcionar se elas funcionarem **bet boo** todos os lugares, uniformemente. Elas reconhecem que não serão as melhores no cross-platform, certo? Nós somos capazes de armazenar chaves de acesso e usá-las **bet boo** todas as superfícies. Não é apenas um benefício de segurança, é também um benefício de velocidade: as chaves de acesso permitem que você pule a verificação de email e a configuração de senha, portanto, é uma experiência melhor para o usuário."

É importante acertar isso, porque "identidade" vai ficar muito mais confusa. Tome as especulações do CEO da Zoom:

> Zoom users in the not-too-distant future could send AI avatars to attend meetings in their absence, the company's chief executive has suggested, delegating the drudge-work of corporate life to a system trained on their own content.

Na prática, um sistema assim está muito longe da realidade. Ou, pelo menos, se realmente tivermos sistemas de IA que possam atender meaningfulmente a uma reunião **bet boo** seu lugar, então as chamadas do Zoom estarão muito longe da lista de coisas que seriam radicalmente alteradas.

Mas sistemas de IA que possam desempenhar a parte de você o suficiente para enganar as

pessoas por um pouco são muito reais. O sistema de síntese de voz mais recente da OpenAI não está publicamente disponível, porque a empresa acha que **bet boo** capacidade de bandeira - imitar convincentemente uma voz com apenas 15 segundos de áudio de amostra - é muito perigosa para ser amplamente disponível. Mas ela sabe que não pode deter a maré por muito tempo e está divulgando o que a tecnologia pode fazer para tentar promover metas de segurança que ela vê como necessárias:

- *Fasear a autenticação baseada **bet boo** voz como medida de segurança para o acesso às contas bancárias e outras informações sensíveis*
- *Explorar políticas para proteger o uso das vozes das pessoas **bet boo** IAs*
- *Educar o público **bet boo** geral sobre as capacidades e limitações das tecnologias de IA, incluindo o conteúdo de IA enganoso*

Como eu disse: se estivermos falando sobre senhas, inteligência Apple ou inteligência artificial, tudo volta à identidade no final. Como posso provar que sou quem digo que sou? Como mesmo posso provar que sou um "eu" **bet boo** primeiro lugar? Independentemente de onde terminarmos indo, uma senha de 16 caracteres simplesmente não vai cortar.

Seis pessoas, incluiendo uma mulher chinesa, foram mortas **bet boo** ataque **bet boo** Sydney

A australiana Yixuan Cheng foi confirmada como a sexta pessoa morta **bet boo** uma série de facadas **bet boo** Bondi Junction, no sábado. A polícia está agora investigando o caso como um suposto ataque targetando mulheres. Cheng, uma estudante chinêsa de aproximadamente 20 anos da Universidade de Sydney, foi uma das vítimas. Cinco mulheres e um homem foram mortos no sábado por Joel Cauchi, de Queensland. Além disso, doze pessoas ficaram feridas, incluindo um bebê. A polícia confirmou que oito das vítimas feridas eram mulheres.

Tabela de Vítimas

Idade	Sexo	Origem	Status
20s	Feminino	China	Falecida
...	...	...	...

Lista de Vítimas

1. Yixuan Cheng (falecida)
2. ...
3. ...

Detalhes do Atacante

Nome
: Joel Cauchi

Idade
: ...

Origem
: Queensland, Australia

Status
: Preso

Informações do documento:

Autor: symphonyinn.com
Assunto: bet boo
Palavras-chave: **bet boo - symphonyinn.com**
Data de lançamento de: 2024-08-23