ИСПОЛЬЗУЕМ USB-ТОКЕНЫ ДЛЯ АУТЕНТИФИКАЦИИ В БРАУЗЕРЕ

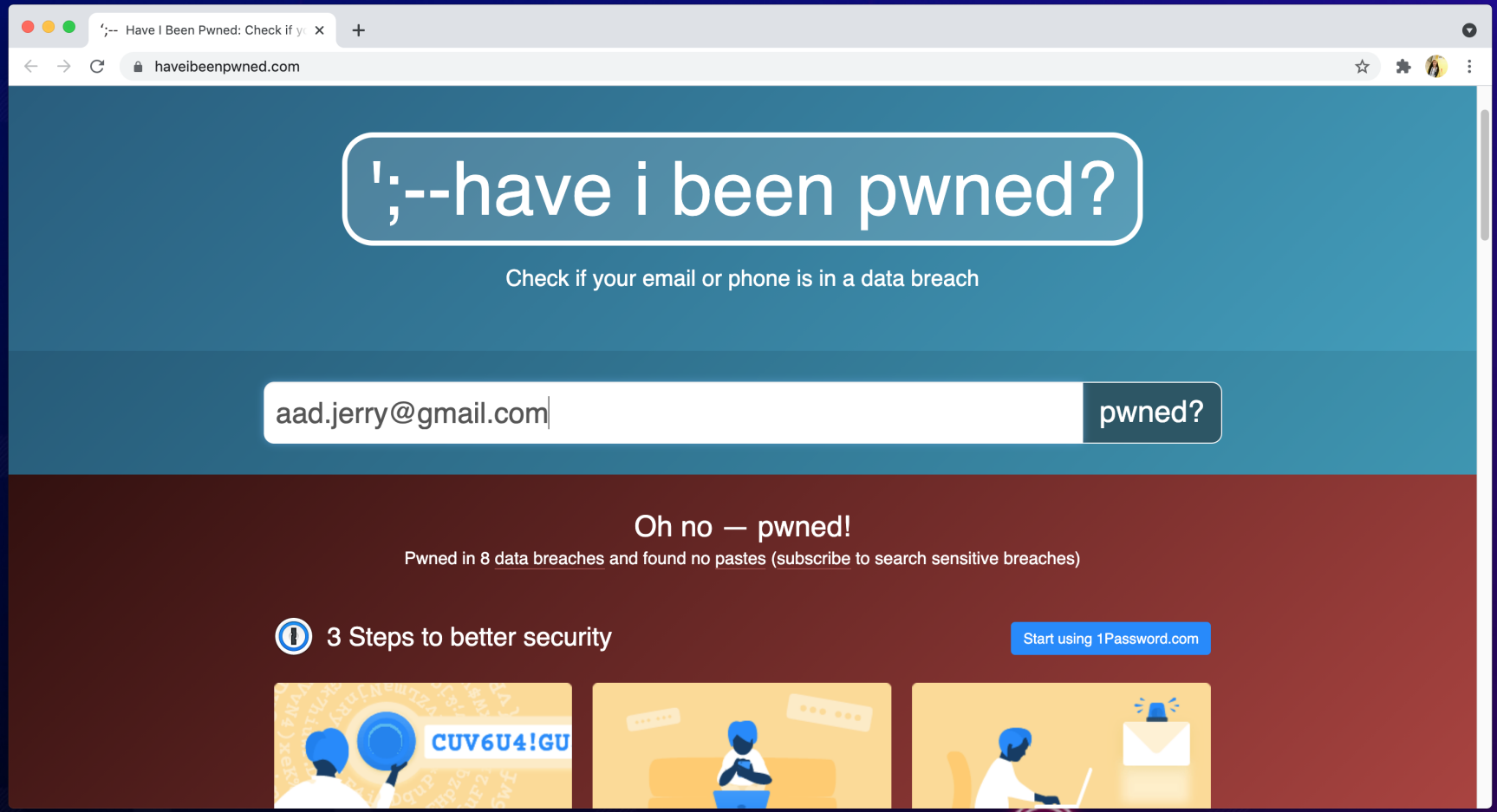
Алексей Авдеев, Mish.Design

👨‍💻 О себе

1. 👨 Алексей Авдеев (https://twitter.com/avdeev_alexey)
2. 👔 CTO, руковожу разработкой
3. 🌆 Из Нижнего Новгорода, работаю в Москве
4. 🌐 Mish.Design
5. 👴 Программирую с 2002 года

Пароли уязвимы

1960

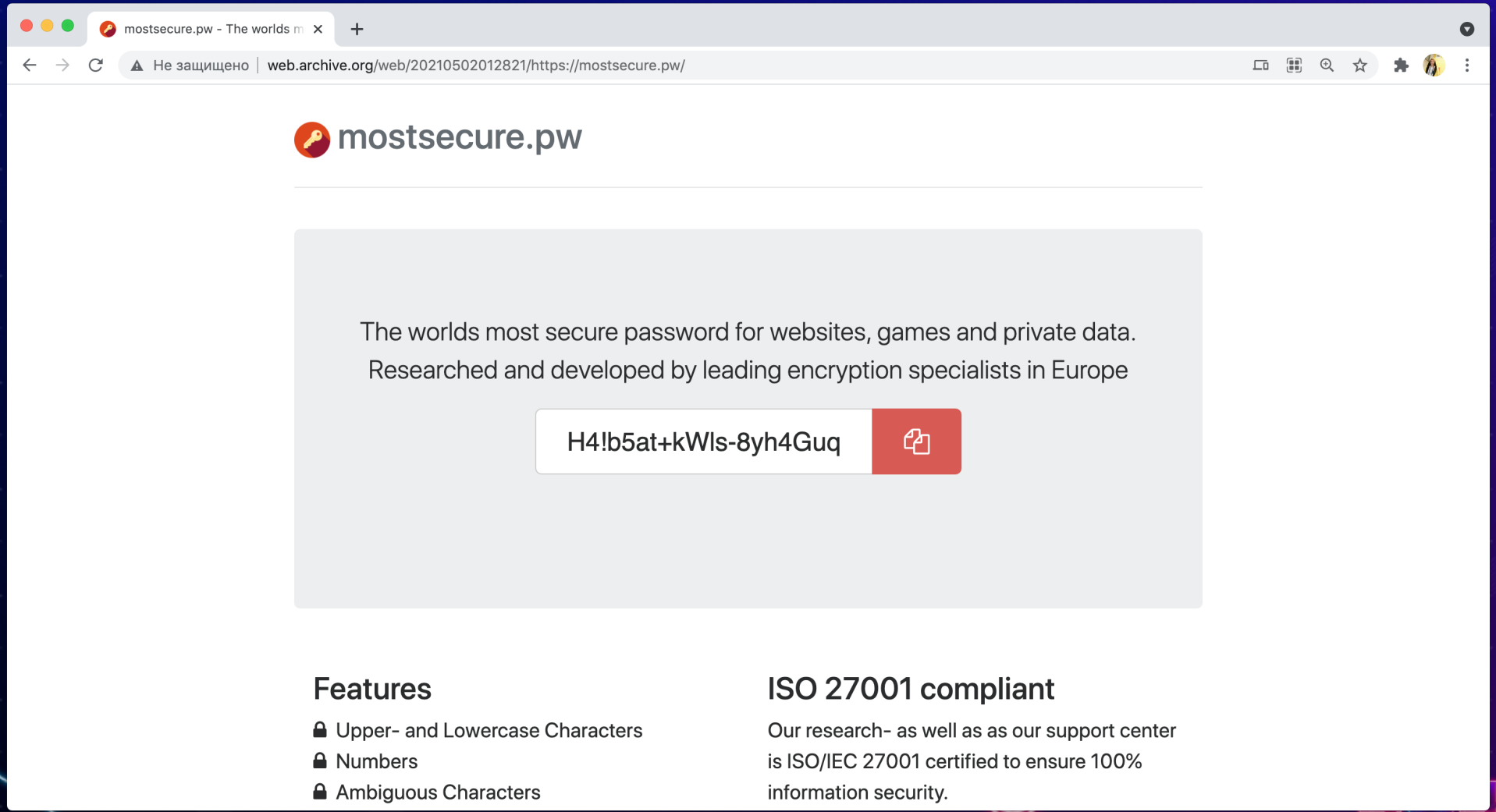

';-- Have I Been Pwned: Check if y
haveibeenpwned.com
';--have i been pwned?
Check if your email or phone is in a data breach
aad.jerry@gmail.com
pwned?
Oh no — pwned!
Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)
3 Steps to better security
Start using 1Password.com
CUV6U4!GU

Сбер
@sberbank

В ответ @a_okshus

Да, логин и пароль не чувствительны к регистру, чтобы пользователям было удобнее. Не переживайте, это безопасно.

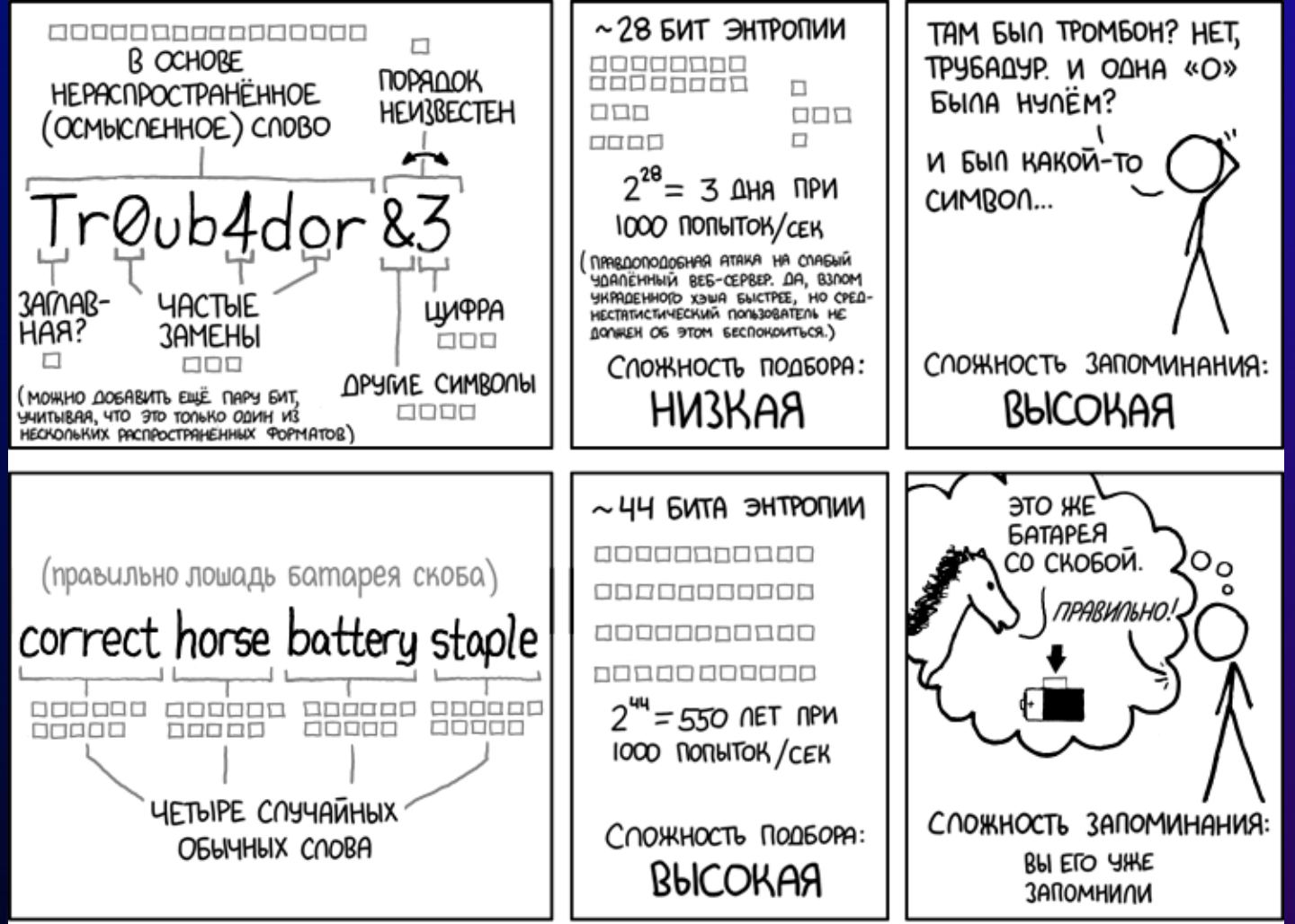
8:36 AM · 7 сент. 2020 г. · Angry.Space


mostsecure.pw - The worlds m
Не защищено | web.archive.org/web/20210502012821/https://mostsecure.pw/
mostsecure.pw
The worlds most secure password for websites, games and private data.
Researched and developed by leading encryption specialists in Europe
H4!b5at+kWls-8yh4Guq
Features
Upper- and Lowercase Characters
Numbers
Ambiguous Characters
ISO 27001 compliant
Our research- as well as as our support center is ISO/IEC 27001 certified to ensure 100% information security.

World Passw*rd Day 2021

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884


ВООБРАЖЕНИЕ КРИПТОМАНЬЯКА:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО! ДАВАЙ ПОСТРОИМ КЛАСТЕР ЗА МИЛЛИОН ДОЛЛАРОВ И ВСЁ ВЗЛОМАЕМ.
НЕ ВЫЙДЕТ – ТАМ 4096-БИТНЫЙ RSA!
ЧЁРТ! НАШ КОВАРНЫЙ ПЛАН СОРВАН!
ЧТО ПРОИЗОШЛО БЫ В РЕАЛЬНОСТИ:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО. ДАЙ ЕМУ НАРКОТЫ И ДУБАСЬ ЭТИМ ГАЕЧНЫМ КЛЮЧОМ ЗА 5 БАКСОВ, ПОКА ОН НЕ СКАЖЕТ ПАРОЛЬ.
ПОНЯЛ.


В ОСНОВЕ НЕРАСПРОСТРАНЁННОЕ (ОСМЫСЛЕННОЕ) СЛОВО
ПОРЯДОК НЕИЗВЕСТЕН
Tr0ub4dor&3
ЗАГЛАВ-НАЯ?
ЧАСТЫЕ ЗАМЕНЫ
ЦИФРА
ДРУГИЕ СИМВОЛЫ
(МОЖНО ДОБАВИТЬ ЕЩЁ ПАРУ БИТ, УЧИТЫВАЯ, ЧТО ЭТО ТОЛЬКО ОДИН ИЗ НЕСКОЛЬКИХ РАСПРОСТРАНЁННЫХ ФОРМАТОВ)
~28 БИТ ЭНТРОПИИ
2^{28} = 3 ДНЯ ПРИ 1000 ПОПЫТОК/СЕК
(ПРАВДОПОДОБНАЯ АТАКА НА СЛАБЫЙ УДАЛЁННЫЙ ВЕБ-СЕРВЕР. ДА, ВЗЛОМ УКРАДЕННОГО ХЭША БЫСТРЕЕ, НО СРЕДНЕСТАТИСТИЧЕСКИЙ ПОЛЬЗОВАТЕЛЬ НЕ ДОЛЖЕН ОБ ЭТОМ БЕСПОКОИТЬСЯ.)
СЛОЖНОСТЬ ПОДБОРА:
НИЗКАЯ
ТАМ БЫЛ ТРОМБОН? НЕТ, ТРУБАДУР. И ОДНА «О» БЫЛА НУЛЁМ?
И БЫЛ КАКОЙ-ТО СИМВОЛ...
СЛОЖНОСТЬ ЗАПОМИНАНИЯ:
ВЫСОКАЯ
(правильно лошадь батарея скоба)
correct horse battery staple
ЧЕТЫРЕ СЛУЧАЙНЫХ ОБЫЧНЫХ СЛОВА
~44 БИТА ЭНТРОПИИ
2^{44} = 550 ЛЕТ ПРИ 1000 ПОПЫТОК/СЕК
СЛОЖНОСТЬ ПОДБОРА:
ВЫСОКАЯ
ЭТО ЖЕ БАТАРЕЯ СО СКОБОЙ.
ПРАВИЛЬНО!
СЛОЖНОСТЬ ЗАПОМИНАНИЯ:
ВЫ ЕГО УЖЕ ЗАПОМНИЛИ
ЗА 20 ЛЕТ СТАРАНИЙ МЫ НАУЧИЛИ ВСЕХ ИСПОЛЬЗОВАТЬ ПАРОЛИ, КОТОРЫЕ ЧЕЛОВЕКУ ЗАПОМНИТЬ СЛОЖНО, А КОМПЬЮТЕРУ ПОДОБРАТЬ ЛЕГКО.

The Consumer Authentication Strength Maturity Model (CASMM) v5

8 PASSLESS

Passwordless *Examples*: WebAuthN, FIDO2

Rather than authenticating with passwords, you authenticate using OS-integrated biometrics.

VULNERABLE TO: SOCIAL ENG / EXTORTION

7 TOKEN2FA

Token-based 2FA *Examples*: OTP Token

In addition to quality passwords in a manager, you authenticate using a physical token that only you have.

VULNERABLE TO: PHISHING

6 APP2FA

App-based 2FA *Examples*: Google Authenticator, Authy

In addition to quality passwords in a manager, you authenticate using an application that only you can access.

VULNERABLE TO: DEVICE COMPROMISE

5 SMS2FA

SMS-based 2FA *Examples*: Any SMS-based auth

In addition to quality passwords in a manager, you authenticate using a text sent to your mobile device.

VULNERABLE TO: SIM-SWAPPING / SMS-HIJACKING

4 PASSMAN

Password Manager *Examples*: 1Password, LastPass

In addition to having unique passwords, you also store them securely in an encrypted archive.

VULNERABLE TO: ACCOUNT RESET / TAKEOVER

3 QUALPASS

Quality Passwords *Examples*: A012-2vOs-11xM

Your passwords are not just unique, but they're long, random, and they include special characters.

VULNERABLE TO: PASSWORD DUMPS / CRACKING

2 UNIQPASS

Unique Passwords *Examples*: DOBs, Teams, Schools

Your passwords are unique, but they're too short, simple, or contain personal information.

VULNERABLE TO: LIVE PASSWORD GUESSING

1 SHARPASS

Shared Passwords *Examples*: Gmail, Wells Fargo, Netflix

You use the same password in multiple places across the internet.

VULNERABLE TO: CREDENTIAL STUFFING

DANIEL MIESSLER 2021

Где решение?


fido™
ALLIANCE
simpler
stronger
authentication

FIDO Authenticator Certification Examples

L3+

USB U2F Token built on a CC-certified Secure Element **Certification: L3+**

L3

USB U2F Token built on a basic simple CPU, OS, is certified. Good physical anti-tampering enclosure

UAF implemented is a TA running on a certified TEE with POP memory

L2

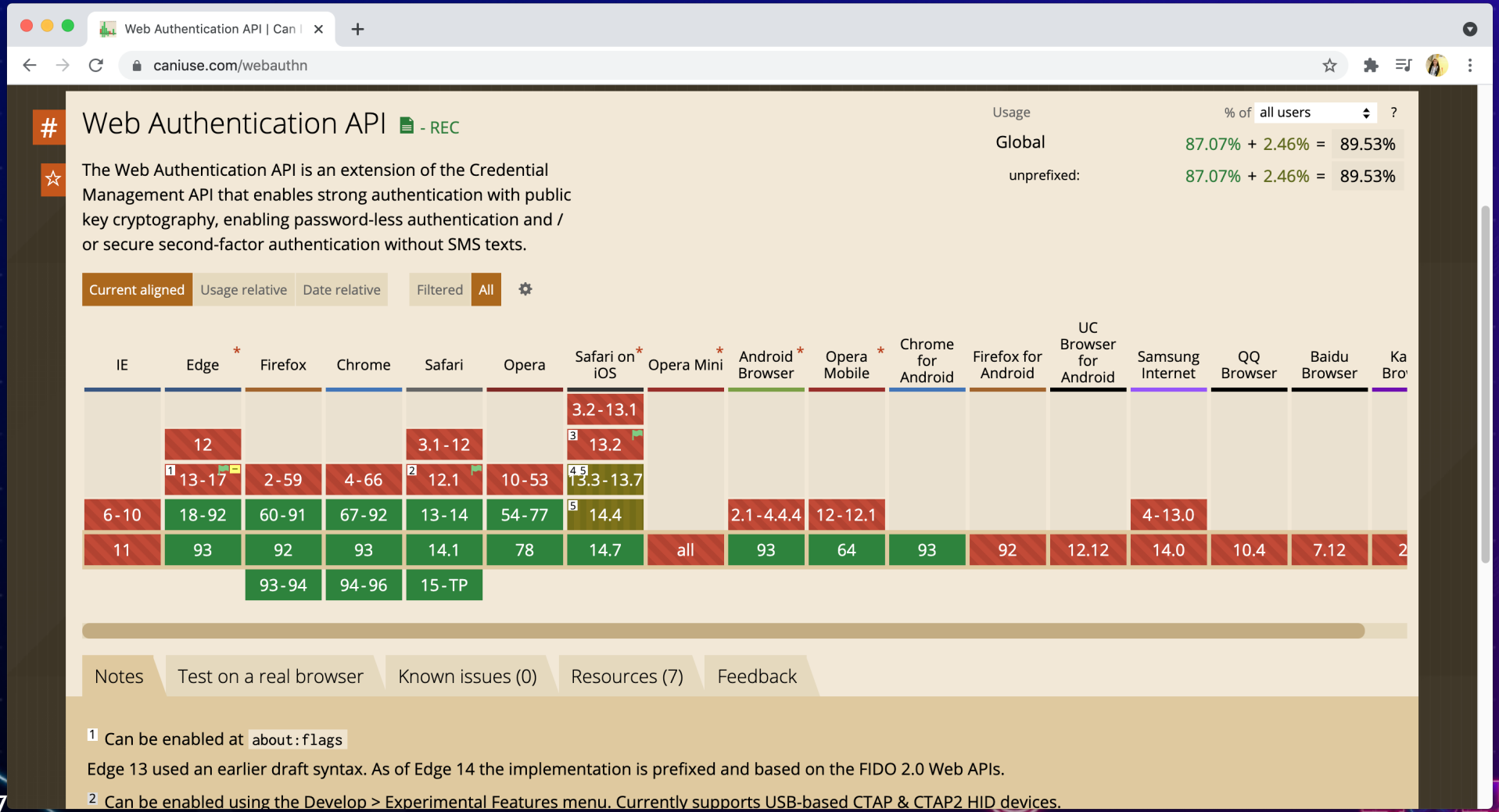
UAF implemented as a TA in an uncertified TEE

L1

Downloaded app making use of Touch ID on iOS
Certification: L1

FIDO2 making use of the Android keystore. Keystore is not certified
Certification: L1

FIDO2 built into a downloadable web browser app
Certification: L1


Web Authentication API | Can
caniuse.com/webauthn
Web Authentication API - REC
The Web Authentication API is an extension of the Credential Management API that enables strong authentication with public key cryptography, enabling password-less authentication and / or secure second-factor authentication without SMS texts.
Usage
% of all users
Global
87.07% + 2.46% = 89.53%
unprefixed:
87.07% + 2.46% = 89.53%
Current aligned
Usage relative
Date relative
Filtered
All
IE
Edge
Firefox
Chrome
Safari
Opera
Safari on iOS
Opera Mini
Android Browser
Opera Mobile
Chrome for Android
Firefox for Android
UC Browser for Android
Samsung Internet
QQ Browser
Baidu Browser
3.2-13.1
12
3.1-12
13.2
13-17
2-59
4-66
12.1
10-53
13.3-13.7
6-10
18-92
60-91
67-92
13-14
54-77
14.4
2.1-4.4.4
12-12.1
4-13.0
11
93
92
93
14.1
78
14.7
all
93
64
93
92
12.12
14.0
10.4
7.12
93-94
94-96
15-TP
Notes
Test on a real browser
Known issues (0)
Resources (7)
Feedback
1 Can be enabled at about:flags
Edge 13 used an earlier draft syntax. As of Edge 14 the implementation is prefixed and based on the FIDO 2.0 Web APIs.
2 Can be enabled using the Develop > Experimental Features menu. Currently supports USB-based CTAP & CTAP2 HID devices.

Закрепленный твит

The FIDO Alliance
@FIDOAlliance

Wondering about the relationship between #FIDO and WebAuthn? A good rule of thumb to remember is FIDO2 = the #WebAuthn + CTAP protocols. 1/4

Перевести твит

9:28 PM · 5 июн. 2020 г. · Twitter Web App

Улучшим пароли

Сложные пароли

Одноразовый пароль

SMS-based

SMS-based

- Не приходят
- Стоят денег
- Можно перехватить

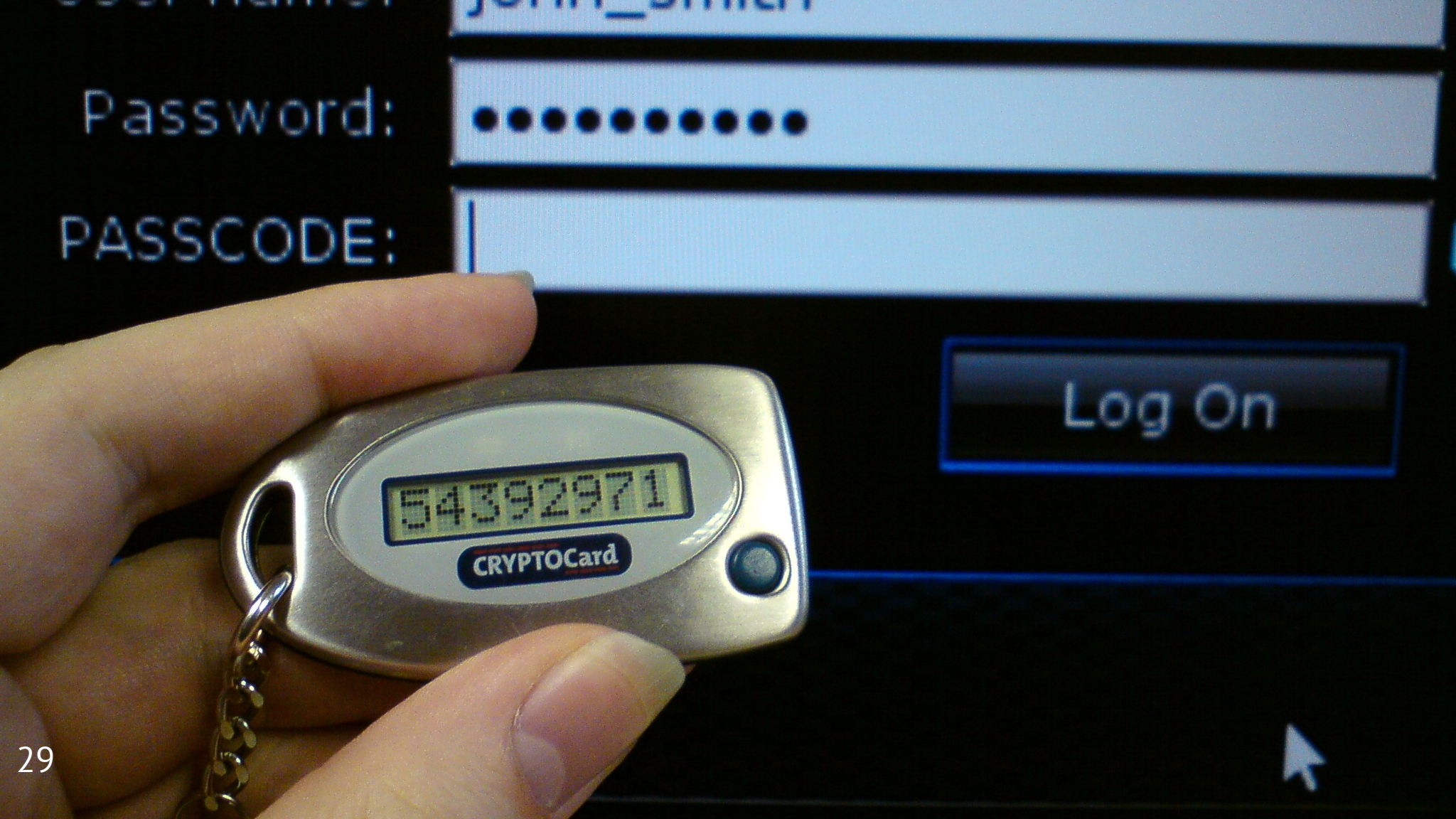
PUSH-код

Двухфакторная аутентификация

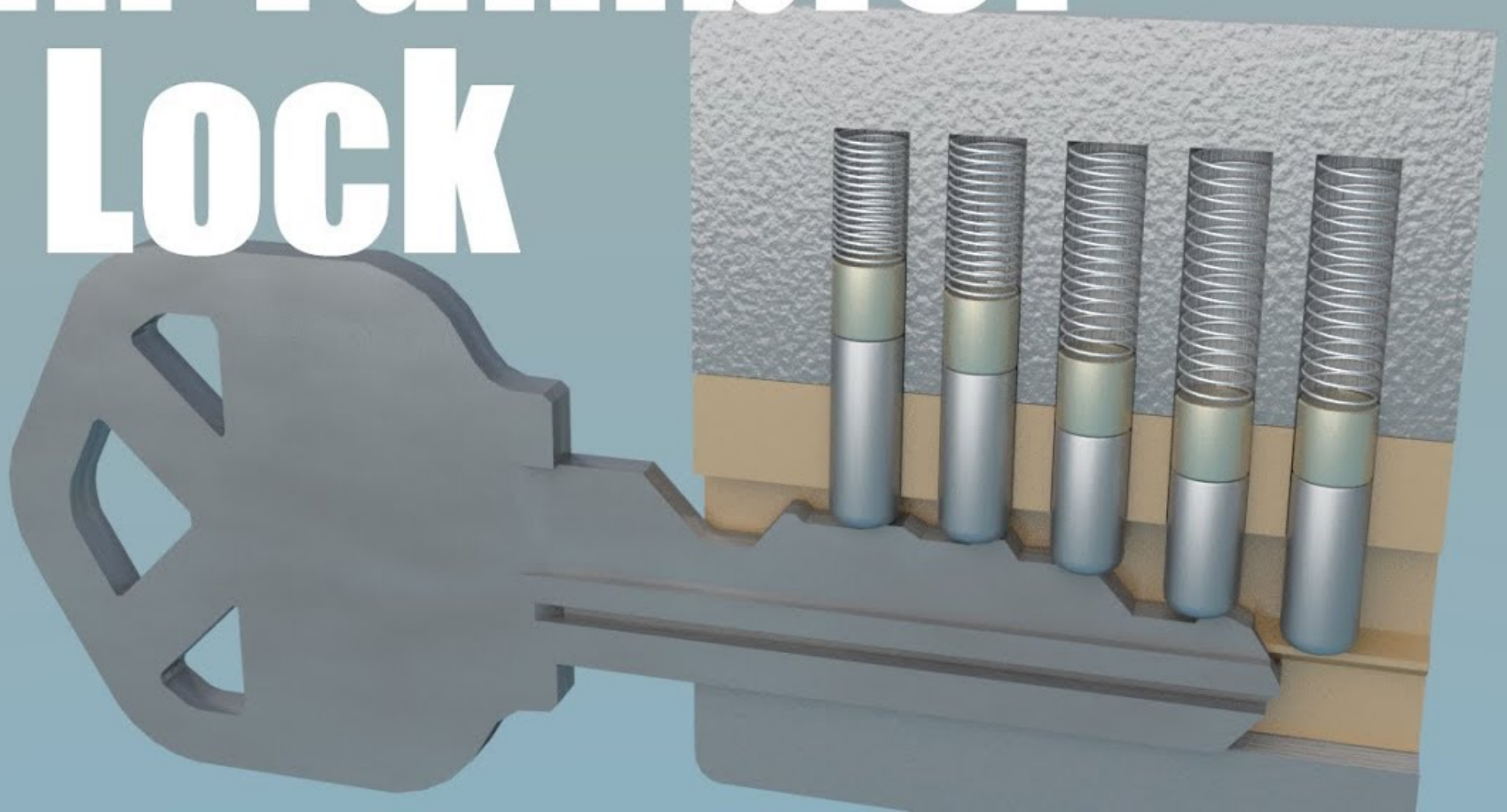
OTP-код

Правила компьютерной безопасности

- не используйте компьютер
- не включайте компьютер
- не владейте компьютером


Password:
PASSCODE:
Log On
54392971
CRYPTOCard

Pin Tumbler Lock



WebAuthn

Демо

Проблемы

Простая безопасная аутентификация

👏 Спасибо!

- 👨 Алексей Авдеев
- 🌐 https://github.com/avdeev
- 🌐 https://twitter.com/avdeev_alexey
- 🌐 Mish.Design