

Bármilyen más, ami biztonságosabb a jelszónál?

Csordás Szilárd

IT biztonsági tanácsadó

November 10



Security Risks Persist with Traditional MFA













of breaches leverage stolen or weak passwords

Compromised credentials remain a major security risk. Tokens and one-time passwords are not user friendly

';--have i been pwned?

561	11,595,834,754	114,132	207,749,077
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

	772,904,991	Collection #1 accounts
	763,117,241	Verifications.io accounts
	711,477,622	Onliner Spambot accounts
	622,161,052	Data Enrichment Exposure From PDL Customer accounts
	593,427,119	Exploit.In accounts
	509,458,528	Facebook accounts
	457,962,538	Anti Public Combo List accounts
	393,430,309	River City Media Spam List accounts
	359,420,698	MySpace accounts
	268,765,495	Wattpad accounts

Password recommendation

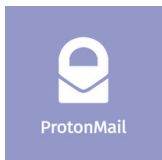


Password guidelines for administrators

Maintain an **8**-character minimum length requirement



Long passwords are stronger, so make your password at least **12** characters long



If you're using a password composed of random characters, about **15** should put it out of reach of modern computing capabilities.





DEPARTMENT OF DEFENSE
PASSWORD MANAGEMENT
GUIDELINE

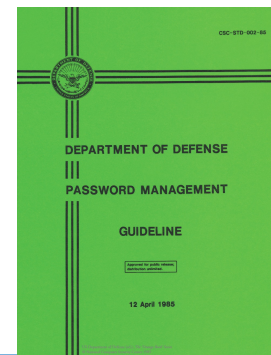
Approved for public release;
distribution limited.

12 April 1985

DEPARTMENT OF DEFENSE
COMPUTER SECURITY CENTER
Fort George G. Meade, Maryland 20755

CSC-STD-002-85
Library No. S-226,994

4.2.1 Security Awareness
4.2.2 Changing Passwords
4.4.1 Single Guess Probability
4.3.3 Transmission
4.3.4 Login Attempt Rate
4.3.5 Auditing
APPENDIX C: **Determining Password Length**



The problem is to determine the needed password length to **reduce to an acceptable level** the probability that a password will be guessed during its lifetime.

...

Experiments on the network have determined that it is possible to make about **8.5 guesses** per minute on the **300-baud** service and **14**, guesses per minute on the **1200-baud** service.

Maximum Lifetime (months)	26-Char alphabet	36-Char alphabet
6	Length of Password	
	9	8

Kevin Mitnic – How Easy It Is to Crack Your Password – 7min

```
OpenCL Platform #1: NVIDIA Corporation
=====
* Device #1: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #2: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #3: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #4: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #5: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #6: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #7: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
* Device #8: GeForce GTX 1080 Ti, 2793/11172 MB allocatable, 28MCU
```



```
Started: Wed Sep 12 03:48:22 2018
Stopped: Wed Sep 12 03:48:53 2018

*****
93397e7a0f2fd5877bd53f389a608d12  ::  qu4dr1l473r4l112*$
*****
```

Stop using passwords – use passphrases! → 24 characters

Always, always use multi-factor authentication!

Use password manager!

Remember, malwares and/or spear-phishing (keylogger) will find a way to compromise the system!

Duo.com

Free up to 10 Users

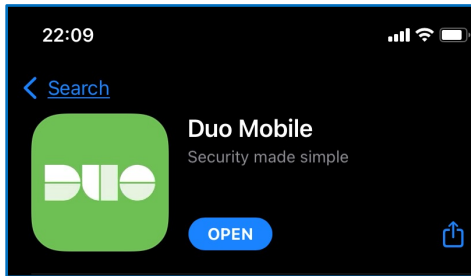
Multi-Factor
Authentication is
the first step!

Protect your workforce with simple, powerful access security.

We're Duo. Our modern access security is designed to safeguard all users, devices, and applications — so you can stay focused on what you do best.

Easy Setup

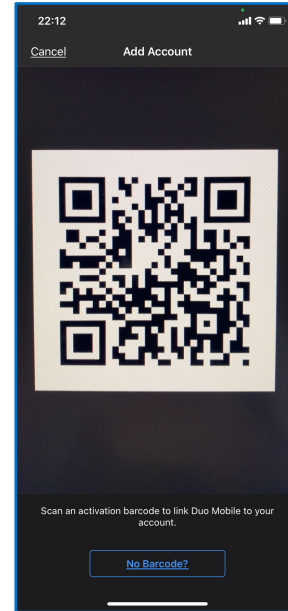
Download it from the
App Store



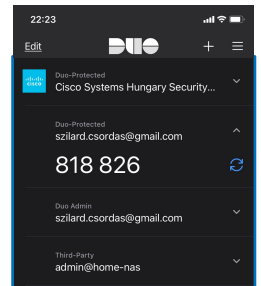
Open the APP



Scan the QRcode



Use it




Any website/APP supports MFA

Felhasználónév **Belépés!**

Jelszó **Jelszó-émlékeztető**

2 factor code

Csökkentett biztonság (Mi ez?)


Two-Step Verification

For your security, your admin has requested two step verification.

Please enter the security code from your authenticator app in the field below.

Enter Security Code


Remember me for 30 days

LOG IN SECURELY

[Resend code](#) | [Lost your phone?](#)

QNAP Store (Update:1 | Installed:15)


Update:1



Media Streaming add-Entertainment

Update

Installed:15



Open

Options


Profile SSH Keys Wallpaper **2-step Verification** Password Settings E-mail Acc

2-step Verification adds an extra layer of protection to your account by requiring an additional one-time security code whenever you sign in to your NAS. For this function, you need a mobile device capable of running an authenticator app.

Status: **Enabled**


Account: admin@home-nas

Security Key: SAF ASOGC




Stop **Reconfigure 2-step Verification**

Apply



Enter your verification code

Use your code generator app to generate a code and enter it below.

 **Szilard Csordas**
@SzilardCsordas

Enter code

[Choose a different verification method](#)

[Contact Twitter Support](#)

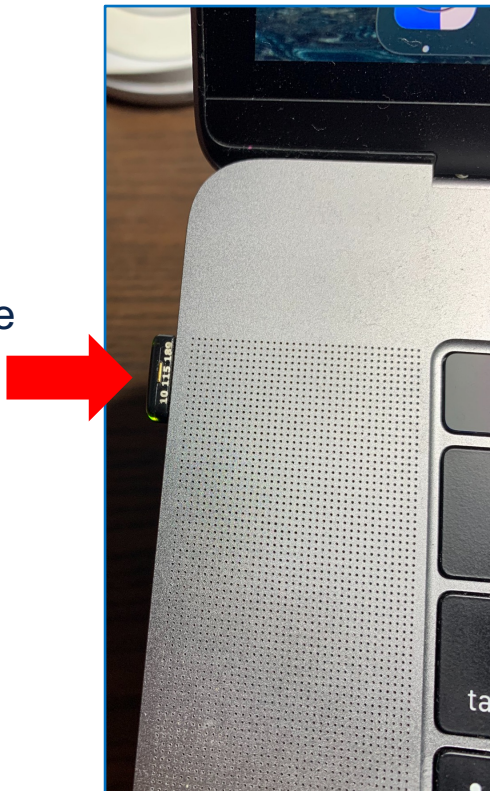
Next



Universal 2nd Factor (U2F)

YubiKey

- created by FIDO
- tamper-proof (SE)
- no spec driver needed
- only tap a physical device



Fast IDentity Online (FIDO2)



- Open standard
- Cryptographic login credentials are **unique** across every website
- **never leave** the user's device and are never stored on a server.
- Users unlock credentials with **fingerprint** readers or **cameras** on their devices, or by leveraging easy-to-use FIDO **security keys**
- Biometric data, when used, never leaves the user's device.

webauthn.io/dashboard

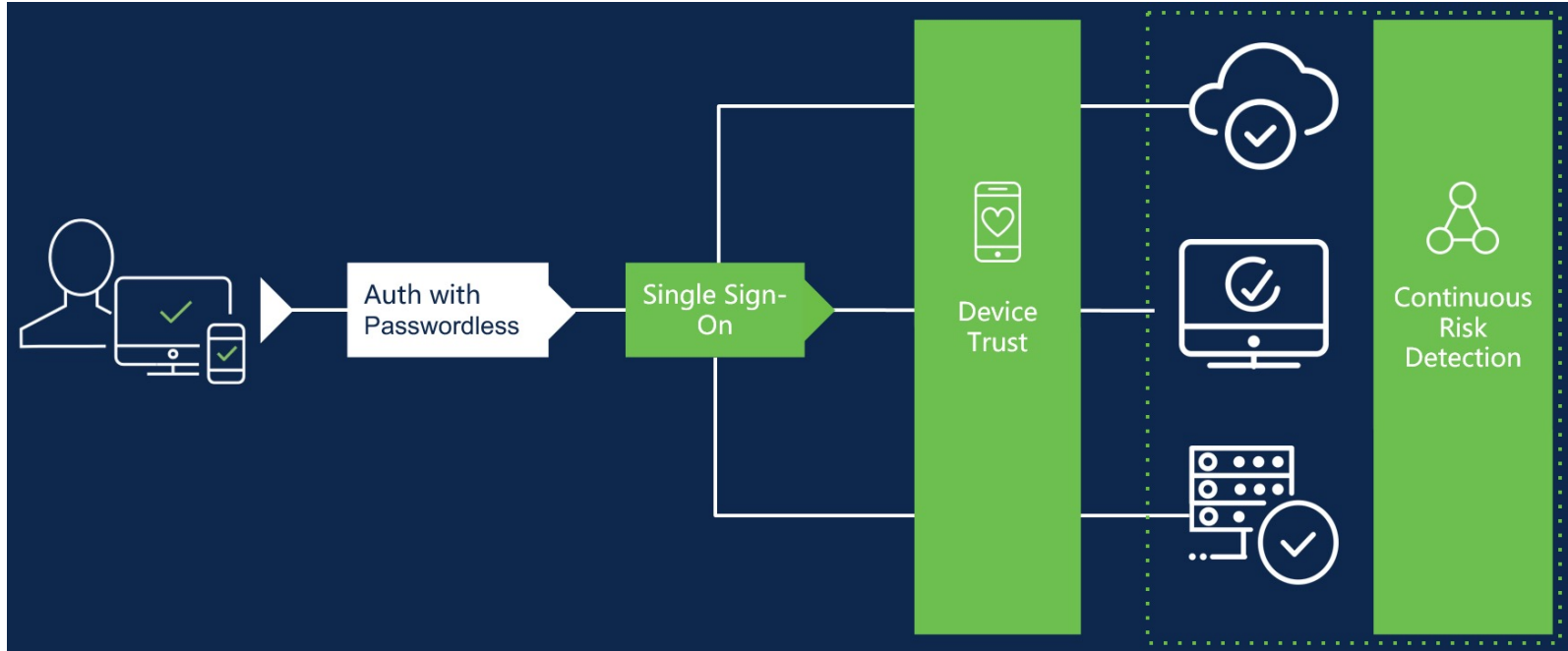
WebAuthn.io

You're logged in!

You just logged in using Web Authentication. Instead of using a traditional, shared-key password, you used a piece of secure hardware to create a strong, attested, and scoped credential that is virtually unphishable! To keep learning about Web Authentication and the FIDO2 framework, check out [webauthn.guide](#).

Try it again?

Continuous trusted access





SECURE