TWO FACTOR AUTHENTICATION AND PASSWORD MANAGERS

STEPHEN GOINS KD9UMZ 11-21-2023

TOPICS

- WHAT IS IT?
  - MULTI-FACTOR AUTHENTICATION
  - NOT TO BE CONFUSED WITH… (2 STEP VERIFICATIONS)
  - SOFTWARE TOKEN APPS
- WHY DO WE NEED IT?
  - PROBLEMS WITH PASSWORDS
  - RECENT HEADLINES
- HOW DO WE IMPLEMENT IT?
  - PASSWORD STANDARDS
  - ADDING TWO-FACTOR

MULTI FACTOR AUTHENTICATION

Three items make up Multi factor authentications

- Something you know
- Something you have
- Something you are

AUTHENTICATION FACTORS

- Something you know
  - Password
  - Pin number
  - Security questions

Answer your security questions

You must verify your identity before making certain changes to your account.

What was your childhood nickname?

answer

What was the name of your first manager?

answer

Forgot your answers? Reset your security questions.

Cancel | Continue

AUTHENTICATION FACTORS

- Something you have

  - Connected token – example Yubikey

  https://www.yubico.com/

AUTHENTICATION FACTORS

- Something you are – biometrics
  - Fingerprint
  - Voice
  - Face recognition
  - Retina/iris

NOT TO BE CONFUSED WITH…

- Two-step verification – one time passwords (OTPS)
  - This is an extra measure of security past a typical login
  - One time password sent via email
  - Can be compromised by man-in-the-middle attack
    - For example, security codes texted to a cell phone

SOFTWARE TOKEN APPS

- Authy and Google Authenticator apps
  - Provides 6-digit TOTPs (time based one time passwords) and has multi-device support
  - Available as a browser extension
  - A sharerd secret key is exchanged during setup between server and app usually via QR code scan
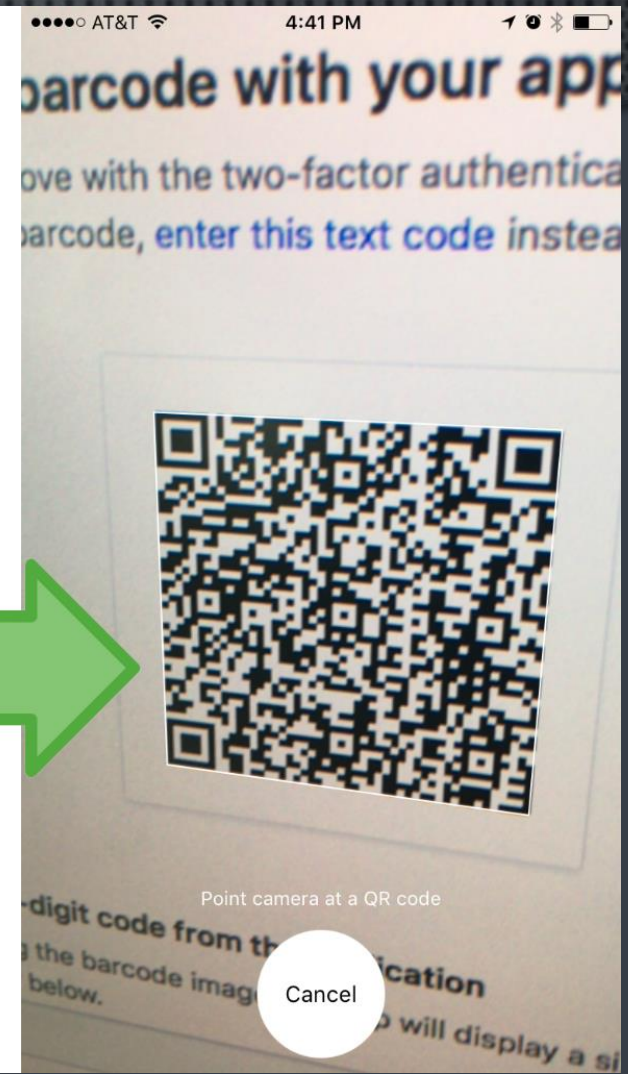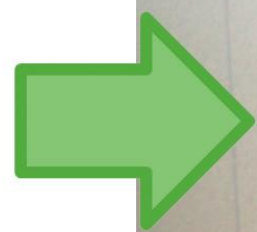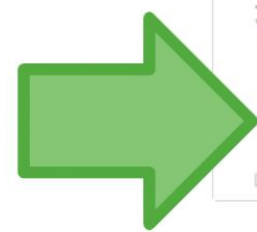 - Available for iOS or Android – authy only

- I recommend using Authy

  - Multi-device support

  - Encrypted backups

  - Can be used all places google authenticator is recommended

  - Easy to use

PROBLEM WITH PASSWORDS

- PASSWORD HELL...

RECENT HEADLINES

- HTTPS://TECH.CO/NEWS/DATA-BREACHES-UPDATED-LIST

- According to this website in 2023 alone there have been 50 breaches so far.

THE (REAL) PROBLEM WITH PASSWORDS

- Ease of sharing and reuse

- Prone to attacks – phishing, malware and brute force

- Complex passwords are often written down

- Creates a single point of failure without 2FA or MFA

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

PASSWORD STANDARDS

Password Requirements

✗ MUST contain at least 8 characters (12+ recommended)
✗ MUST contain at least one uppercase letter
✗ MUST contain at least one lowercase letter
✗ MUST contain at least one number
✗ MUST contain at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)
✔ MAY NOT contain more than two identical characters in a row
✔ MAY NOT contain first name, last name, email address mailbox or domain, company name or commonly used passwords
✔ MAY NOT match commonly used password character patterns

 5 remaining rules need to be met

create a very strong password for me

PASSWORD MANAGERS (VAULTS)

There are many password managers out there that can be used. I have decided to go with Bitwarden.

- Ease of use
- Multi-device compatibility
- Generates and stores passwords or pass-phrases
- Browser extension and quick fills website login info
- Can store your credit card info
- One strong password to remember and you have access to all passwords.
- Multi factor authentication (authy, yubikey, biometrics)

MISC

- Authy - https://authy.com/

- Bitwarden - https://bitwarden.com/

- Vpn security (private internet access "pia" or express vpn)

  - Express vpn is easier to use than PIA.

  - https://www.expressvpn.com/

  - https://www.privateinternetaccess.com/

- Choice of web browsers – brave - https://brave.com/

  - Has built in blockers for tracking and web ads

- Yubico Hardware key - https://www.yubico.com/