Mateusz Czerniawski

Have I been pwned?

Arcontar

This session

- Logins and Passwords
- You’ve been pwned!
- Password policy
- MFA
- PasswordLess

Login

- Each login is the gateway to your online identity!

Login

You'll never have more ideas about how to protect your identity than the minute after you realise it's been stolen!

Arcontar

Login

- Ojciec oszukał mnie przez FB

https://niebezpiecznik.pl/post/ojciec-oszukal-mnie-przez-facebooka-czyli-dwa-ataki-swietnie-przygotowanego-zlodzieja-z-kryptowalutami-w-tle/

Login

- Ojciec oszukał mnie przez FB

https://niebezpiecznik.pl/post/ojciec-oszukal-mnie-przez-facebooka-czyli-dwa-ataki-swietnie-przygotowanego-zlodzieja-z-kryptowalutami-w-tle/

- Zakupy na Morele

https://zaufanatrzeciastrona.pl/post/uwaga-na-duza-fale-atakow-udajacych-posrednikow-szybkich-platnosci/

Login

- Ojciec oszukał mnie przez FB

https://niebezpiecznik.pl/post/ojciec-oszukal-mnie-przez-facebooka-czyli-dwa-ataki-swietnie-przygotowanego-zlodzieja-z-kryptowalutami-w-tle/

- Zakupy na Morele

https://zaufanatrzeciastrona.pl/post/uwaga-na-duza-fale-atakow-udajacych-posrednikow-szybkich-platnosci/

- Przez pocztę do karty SIM I przejęcia konta bankowego

https://niebezpiecznik.pl/post/przestepcy-przekierowali-mu-telefon-i-okradli-konto-w-banku/

Passwords

Passwords

2007

The average user has 6.5 passwords, each of which is shared across 3.9 different sites.

http://research.microsoft.com/en-us/um/people/cormac/papers/www2007.pdf

Passwords

2007

The average user has 6.5 passwords, each of which is shared across 3.9 different sites.

2007

The average user has about 25 accounts that require passwords, and types an average of 8 passwords per day

http://research.microsoft.com/en-us/um/people/cormac/papers/www2007.pdf

Passwords

2007

The average user has 6.5 passwords, each of which is shared across 3.9 different sites.

2007

The average user has about 25 accounts that require passwords, and types an average of 8 passwords per day

2017

”We found the average employee using LastPass is managing 191 passwords”

http://research.microsoft.com/en-us/um/people/cormac/papers/www2007.pdf
https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html

Arcontar

Passwords

2007

The average user has 6.5 passwords, each of which is shared across 3.9 different sites.

2007

The average user has about 25 accounts that require passwords, and types an average of 8 passwords per day

2017

"We found the average employee using LastPass is managing 191 passwords"

2018

81% of confirmed data breaches are due to passwords.

http://research.microsoft.com/en-us/um/people/cormac/papers/www2007.pdf
https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html
https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords

Arcontar

Passwords

Attack	Frequency	Difficulty	User assists attacker by …	Password matter?
Credential Stuffing	Very high	Very easy	Password reuse	No
Phishing	Very high	Easy	Click links	No
Keystroke logging	Low	Medium	Click link, run as Admin	No
Local discovery	Low	Difficult	Writing passwords	No
Extortion	Very low	Difficult	Fear for relatives	No
Password spray	Very high	Trivial	Password reuse	No
Brute force	Very low	Varies	None	Yes – if using unguessable

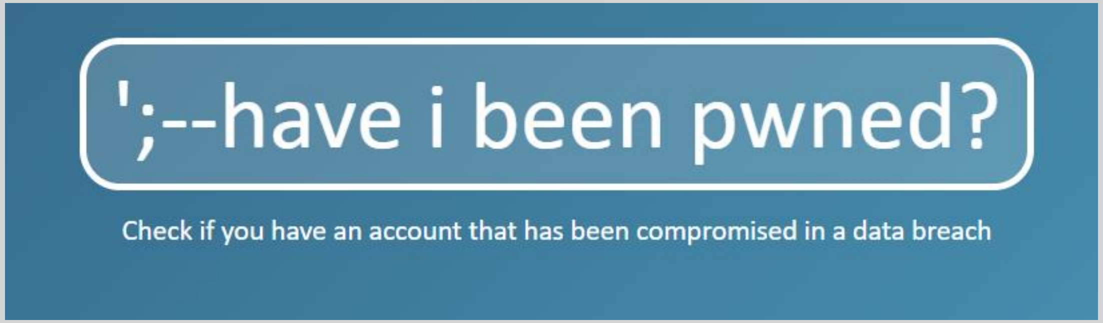
https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984

Arcontar

You’ve been pwned!

- ***Pwned***, simply means that your account has been the victim of a data breach
- A "breach" means when YOUR data is EXPOSED!
- Data leaks happen! https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Demo



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Arcontar

Password reusability

- KeePass (257/240/~100)
- LastPass
- 1Password

Arcontar

Password reusability

SINGLE PASSWORD = MULTIPLE ACCOUNTS AFFECTED

UNIQUE PASSWORDS = SINGLE ACCOUNT AFFECTED

Password policy

- _Your Password Has Expired and Must Be Changed_

getMEIN2!getMeIn2!***You!

Password policy

- ~~*Your Password Has Expired and Must Be Changed getMEIN2!getMeIn2!***You!*~~

- Conditional Access
- Login Behavioural Analysis
- Tracking Known Devices

Password policy

- Windows 1903 baseline – no more password-expiration policy!

  https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903

- NIST (National Institute of Standards and Technology) guideline

  https://pages.nist.gov/800-63-3/sp800-63b.html

- Hello Windows Hello!

  https://aka.ms/gopasswordless

MFA

Authentication is a method of proving YOU ARE who you say you are

MFA

Authentication is a method of proving YOU ARE who you say you are

- Something you know (a password or PIN code)
- Something you have (an RSA token, smart card or a device)
- Something you are (a fingerprint or retinal scanner)

MFA

Multi-factor authentication is simply using more than one of these methods for access.

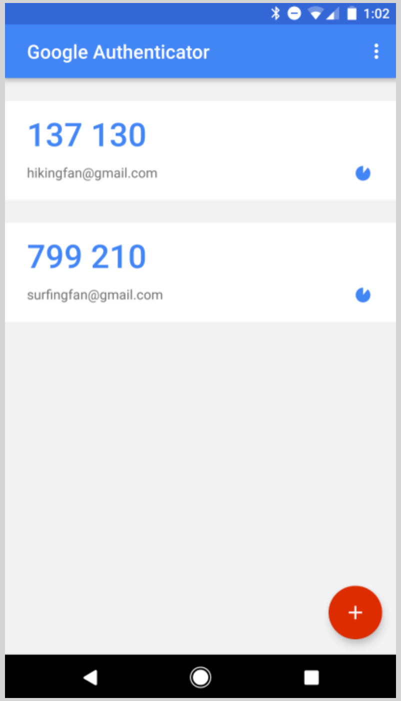
- Something you know (a password or PIN code)
- Something you have (an RSA token, smart card or a device)
- Something you are (a fingerprint or retinal scanner)

MFA

Arcontar

MFA

- OTP – mobile App:
  - Google Authenticator



Google Authenticator

137 130

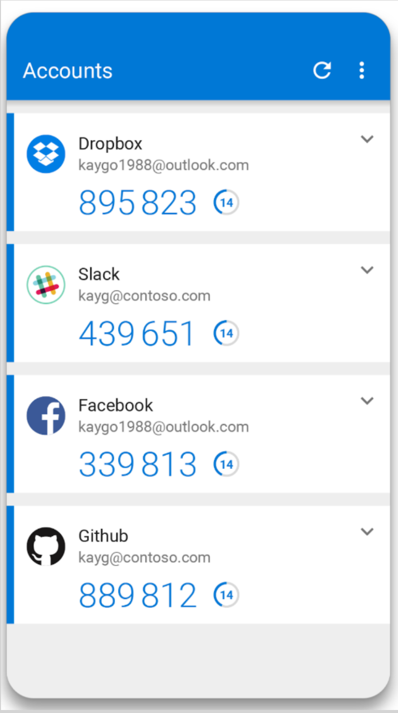
hikingfan@gmail.com

799 210

surfingfan@gmail.com

MFA

- OTP – mobile App:
  - Google Authenticator
  - Microsoft Authenticator



Accounts

Dropbox
kaygo1988@outlook.com
895 823

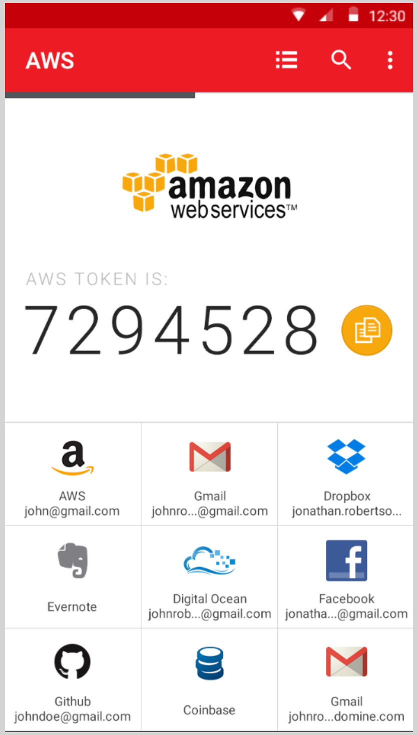
Slack
kayg@contoso.com
439 651

Facebook
kaygo1988@outlook.com
339 813

Github
kayg@contoso.com
889 812

MFA

- OTP – mobile App:
    - Google Authenticator
    - Microsoft Authenticator
    - Authy

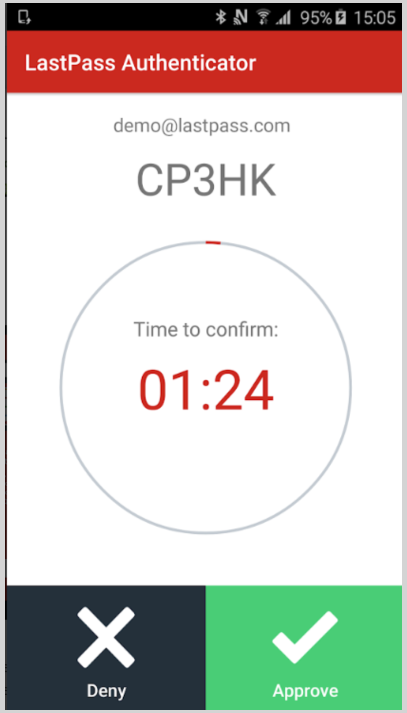


AWS TOKEN IS:

7294528

MFA

- OTP – mobile App:
  - Google Authenticator
  - Microsoft Authenticator
  - Authy
  - LassPass Authenticator



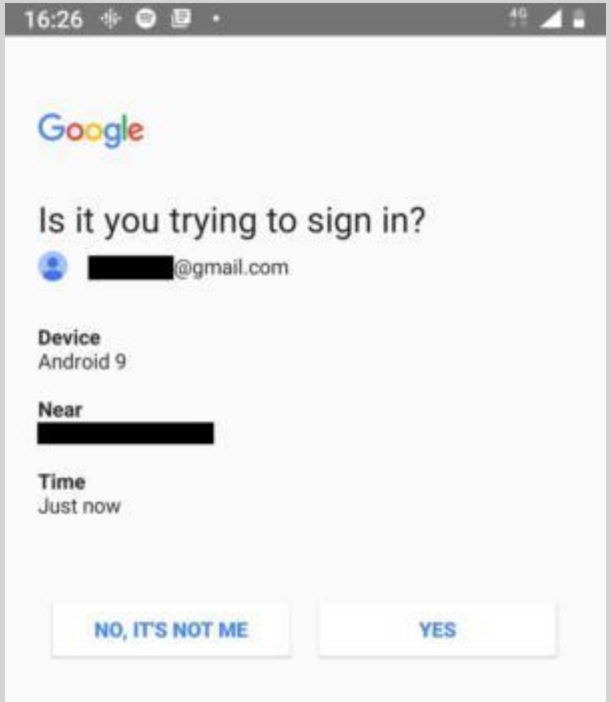
Arcontar

MFA

- OTP – mobile App
- FIDO - Hardware options:
  - Yubico Authenticator

MFA

- OTP – mobile App
- FIDO - Hardware options
- Google on-device prompts



16:26

Google

Is it you trying to sign in?

[redacted]@gmail.com

Device
Android 9

Near
[redacted]

Time
Just now

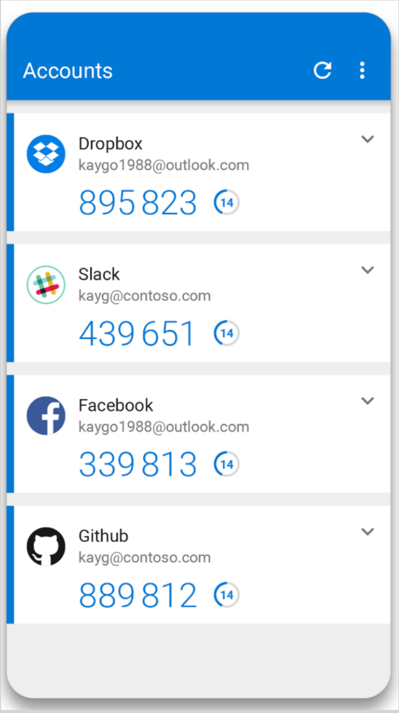
Arcontar

MFA

Login + Password - 📵 = 🔐 🧑‍💻

Arcontar

Demo



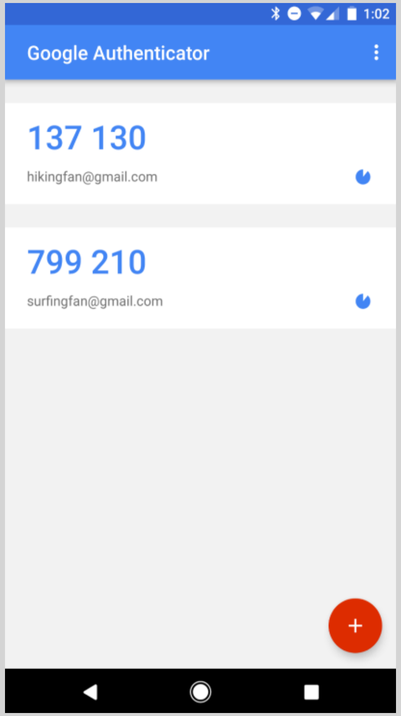
Accounts

Dropbox
kaygo1988@outlook.com
895 823 14

Slack
kayg@contoso.com
439 651 14

Facebook
kaygo1988@outlook.com
339 813 14

Github
kayg@contoso.com
889 812 14



Google Authenticator

137 130
hikingfan@gmail.com

799 210
surfingfan@gmail.com

Stay secure

Enable MFA

https://twofactorauth.org/

Arcontar

about_me

Mateusz Czerniawski

Arcontar

mczerniawski@arcon.net.pl

@Arcontar

www.mczerniawski.pl

mczerniawski