

';--have i been pwned?

**Þetta þarf ekki að vera svona flókið!**



# Um mig

- Stefán Jökull Sigurðarson
- Principal Software Engineer @ Lucinity in Reykjavík
- Microsoft MVP – Developer Technologies síðan 2020
- Have I Been Pwned (hlutastarf)
- <https://stebet.net>

NETFLIX

Oh, the passwords.

 LUCINITY

# Lykilorð eru svo “skemmtileg”

- Þurfa að vera flókin
- Þurfum að breyta þeim reglulega
- Megum ekki nota sum tákni
- Oft ekki hægt að „patea“ í lykilorðareitinn
- Öryggisspurningar ef við lendum í vandræðum

# Flókin lykilorð

password

**Flókin lykilorð**

**Password**

# Flókin lykilorð

Password1

# Flókin lykilorð

Password1!



# Flókin lykilorð

## Breyta lykilorði



Lykilorðið verður að innihalda a.m.k. 10 stafi

Lykilorðið verður að innihalda bæði stóra og litla stafi

Lykilorðið verður að innihalda að minnsta kosti eitt tákni

Lykilorðið verður að innihalda amk eina tölu

Lykilorðið má ekki innihalda fleiri en tvo stafi eða tölur í réttri röð

Lykilorðið má ekki innihalda fleiri en tvo stafi, tölur eða tákni sem eru endurteknir

# Flókin lykilorð

## Breyta lykilorði



Lykilorðið verður að innihalda a.m.k. 10 stafi

Lykilorðið verður að innihalda bæði stóra og litla stafi

Lykilorðið verður að innihalda að minnsta kosti eitt tákn

Lykilorðið verður að innihalda amk eina tölu

Lykilorðið má ekki innihalda fleiri en tvo stafi eða tölur í réttri röð

Lykilorðið má ekki innihalda fleiri en tvo stafi, tölur eða tákn sem eru endurteknir

Password1!



CQSSIP AS9VORD

\*\*\*\*\* 🔒

Creat 0:332L passwrd !

# Réttlættingar



**MBNA**  
@mbna

Hi. I understand your concerns. Our Online Card Services login is our first line of security, but we do have many other hidden security features in place that help us to protect your account and details. ^LauraP



**ING Australia**  
@ING\_Aust

Good morning, Keep in mind with ING a 4 digit access code is the  
... attempts of entering an Access  
... Alissa



**ING Australia**  
@ING\_Aust

Hi Owen, your online banking is safe and secure with ING. We take security seriously, and use industry-leading technology to protect your accounts. Plus, we have an Online Security Guarantee in place. In the unlikely event that an unauthorised...

En er til “rétt” leið?

NILST

# Já!

- NIST Digital Identity Guidelines - SP 800-63
- <https://pages.nist.gov/800-63-4/sp800-63b.html>



# Flókin lykilorð

- Fjöldi rannsókna hafa verið gerðar á kostum og göllum flókinna lykilorða
- Komast flestar að sömu niðurstöðu

# Flókin lykilorð

*“a user that might have chosen “password” as their password would be relatively likely to choose “Password1” if required to include an uppercase letter and a number, or “Password1!” if a symbol is also required.”*



# Flókin lykilorð

*“Users’ password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the “**Password1!**” example above”*

# Flókin lykilorð

*“Users’ password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the “Password1!” example above. **For this reason, it is recommended that passwords chosen by users be compared against a blocklist of unacceptable passwords**”*

# En að breyta reglulega?

- Meiri rannsókir, t.d. hjá FTC, Carleton University, University College London og Carnegie Mellon
- Svipaðar niðurstöður...

# Breyta reglulega

*“Today, attackers who have access to the hashed password file can perform offline attacks and guess large numbers of passwords. The Carleton researchers demonstrate mathematically that frequent password changes only hamper such attackers a little bit, probably not enough to offset the inconvenience to users.”*

# Breyta reglulega

*“The Carleton researchers also point out that an attacker who already knows a user’s password is unlikely to be thwarted by a password change. As the UNC researchers demonstrated, **once an attacker knows a password, they are often able to guess the user’s next password fairly easily.**”*

# Ekki hægt að „patea“ í lykilorðareitinn

*“Verifiers **SHALL** allow the use of password managers. To facilitate their use, verifiers **SHOULD** permit claimants to use “paste” functionality when entering a memorized secret. Password managers may increase the likelihood that users will choose stronger memorized secrets.”*

# Öryggisspurningar


- Notendur velja yfirleitt slakar spurningar sem er auðvelt að muna
- Förum í smá leik!

# Öryggisspurningar





# Öryggisspurningar - dæmi

- **Í hvaða borg/bæ er notandinn fæddur?**
  - Skoðum Facebook
- **Nafn móður?**
  - Skoðum Facebook
- **Æskuvinur?**
  - Skoðum Facebook
- **Fyrsta gæludýr**
  - Skoðum Facebook
- **Eigið val eða skrifa spurninguna sjálfur?**
  - Notandinn skrifar líklega bara lykilorðið 

# Hvernig á þá að meðhöndla lykilorð?

- **Sleppið því (ef það er hægt)!**
  - Notið samfélagsmiðlainnskráningar eins og Google, Microsoft Account, Facebook, Apple ID t.d.
  - Notið aðgangsstýringar eins og Entra/Azure AD, Okta, Auth0
- **En oft er ekki hægt að sleppa þeim**
  - Utanaðkomandi kröfur/reglur
  - Eldri kerfi

# Þetta þarf ekki að vera svona flókið!

- **Minnst 8 stafir**
- **Ekki banna notkun á ákveðnum táknum**
  - Meira að segja emojis ættu að vera velkomin sem tákn í lykilorði 🍌🔒🌐
- **Ekki gera kröfur um flókið lykilorð**
- **Ekki bjóða upp á "vísbendingar" eða öryggisspurningar**
- **Gangið úr skugga um að lykilorðið sé ekki í gagnaleikum**
- **Auðveldið notendum að nota lykilorðageymslur (Password Manager)**
- **Leiðbeinið!**

# Er lykilorðið í gagnaleikum?

- Have I Been Pwned er með API sem er frítt að nota
- <https://haveibeenpwned.com/API/v3#PwnedPasswords>



# Pwned Passwords API

- Yfir 850 milljónir lykilorða (hashes) úr gagnaleikum
- Uppfært reglulega
- Stofnanir eins og FBI (USA) og NCA (UK) hjálpa til - bættu við milljónum lykilorða á síðasta ári



# Hversu oft hefur lykilorðið “Password1!” lekið?

Password1!



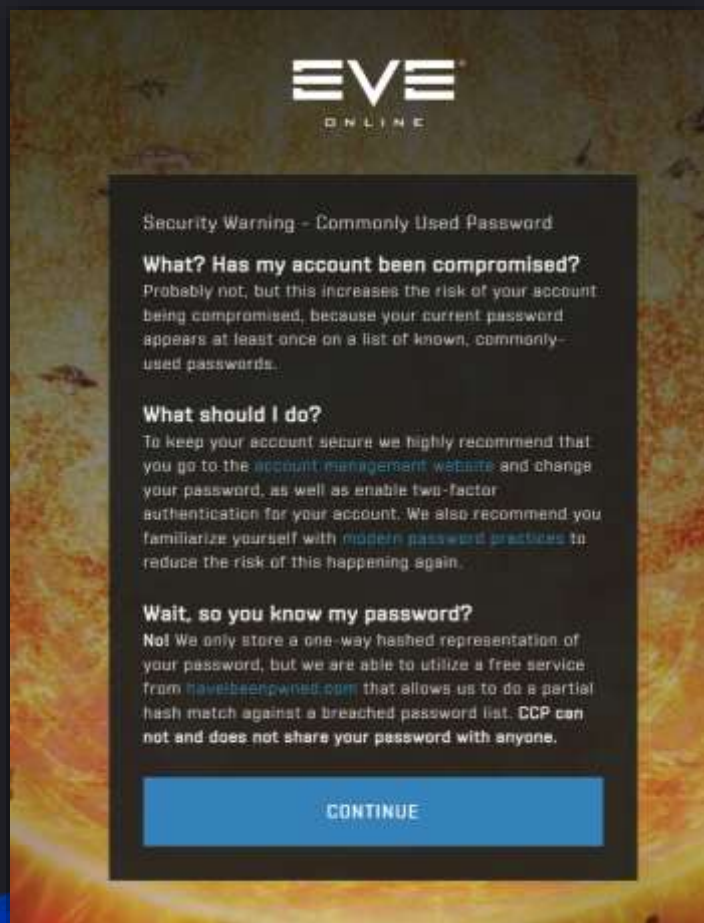
pwned?

Oh no — pwned!

This password has been seen 29,588 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

# Leiðbeinið – dæmi um notkun á Pwned Passwords



**EVE ONLINE**

Security Warning – Commonly Used Password

**What? Has my account been compromised?**  
Probably not, but this increases the risk of your account being compromised, because your current password appears at least once on a list of known, commonly-used passwords.

**What should I do?**  
To keep your account secure we highly recommend that you go to the [account management website](#) and change your password, as well as enable two-factor authentication for your account. We also recommend you familiarize yourself with [modern password practices](#) to reduce the risk of this happening again.

**Wait, so you know my password?**  
No! We only store a one-way hashed representation of your password, but we are able to utilize a free service from [haveibeenpwned.com](#) that allows us to do a partial hash match against a breached password list. CCP can not and does not share your password with anyone.

[CONTINUE](#)



**Watchtower**

Get alerts for any security issues that affect you. Your score gives an overall idea of how safe your data is. Take action on the flagged items to level up your security.

[Share My Score](#)

**1011**  
FANTASTIC

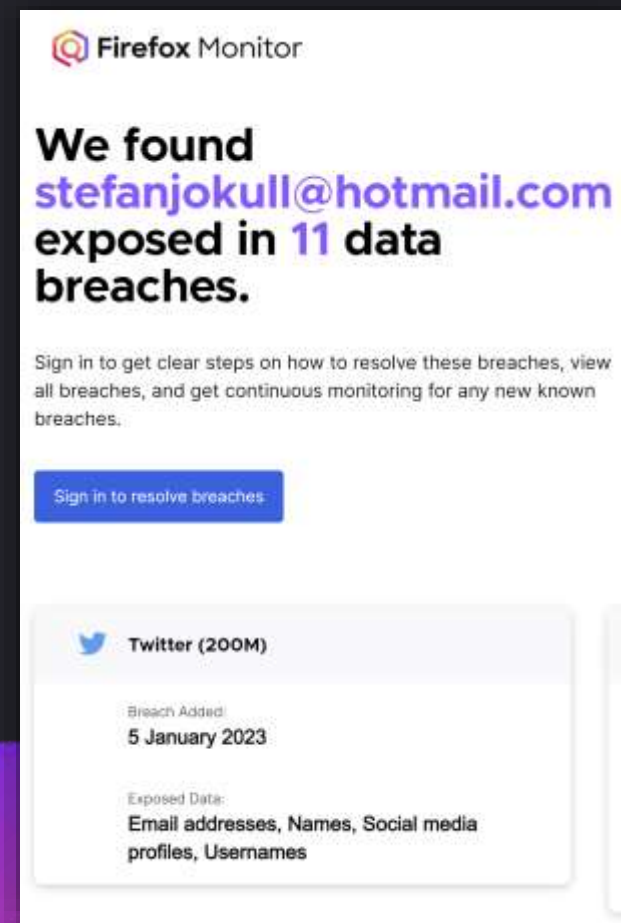
**Overall Password Strength**

**6**  
**Vulnerable Passwords**  
These passwords were found in a database of breached passwords from [haveibeenpwned.com](#). Change them to keep your accounts safe.  
[Show Items](#)

**28**  
**Reused Passwords**  
Don't use the same password on multiple websites. Generate unique passwords to improve your security.  
[Show Items](#)

**14**  
**Weak Passwords**  
Weak passwords are easier to guess. Generate strong passwords to keep your accounts safe.  
[Show Items](#)

**23**  
**Unsecured Websites**  
Websites that use HTTP URLs aren't secure. Try changing the URL to use HTTPS to secure your connection to the site.  
[Show Items](#)



**Firefox Monitor**

**We found [stefanjokull@hotmail.com](mailto:stefanjokull@hotmail.com) exposed in 11 data breaches.**

Sign in to get clear steps on how to resolve these breaches, view all breaches, and get continuous monitoring for any new known breaches.

[Sign in to resolve breaches](#)

**Twitter (200M)**

Breach Added  
**5 January 2023**

Exposed Data:  
**Email addresses, Names, Social media profiles, Usernames**

# Leiðbeinið – dæmi um notkun á Pwned Passwords

PASSWORD

.....



The password you've chosen is not secure and has been identified as risky due to past breaches. Please choose a more secure password.

please. Please choose a more secure password.

The password you've chosen is not secure and has been identified as risky due to past breaches. Please choose a more secure password.



# Ekki þvælast fyrir!

- Leyfið notendum að „patea“ lykilorð
- Ekki koma í veg fyrir að notendur geti notað lyklaborðið og tólin sín, t.d. með sérstökum “skjályklaborðum” (on-screen keyboards)

## Access Your TreasuryDirect Account

[? Learn more about Security Features and Protecting Your Account.](#)

Use your standard keyboard to enter your Account Number.

Account Number:

Use your mouse to enter your Password on the virtual keyboard below and click "Enter".

Password:  (Password is not case sensitive.)

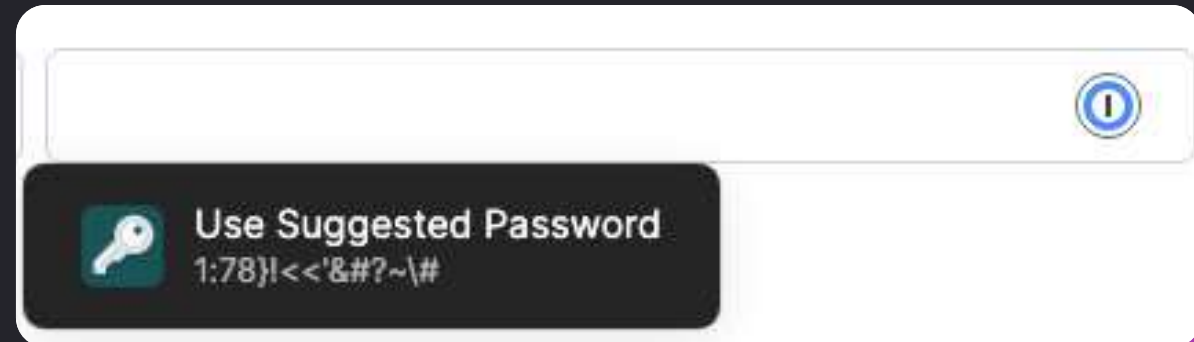
A [virtual keyboard](#), with keys that display in random order, is available to deter others from learning your password.



[Enter](#) [Forgot your Account Number?](#) [Forgot your Password?](#)

# passwordrules eigindi

- <https://developer.apple.com/password-rules/>
- HTML eigindi sem lýsir lykilorðakröfum
- Hjálpar lykilorðageymslum að búa til gild lykilorð
- Dæmi:
- `<input type="password" ... passwordrules="min-length: 12">`
- Margir möguleikar, t.d. :
  - required: upper;
  - required: lower;
  - allowed: ascii-printable;
  - minlength: 12;



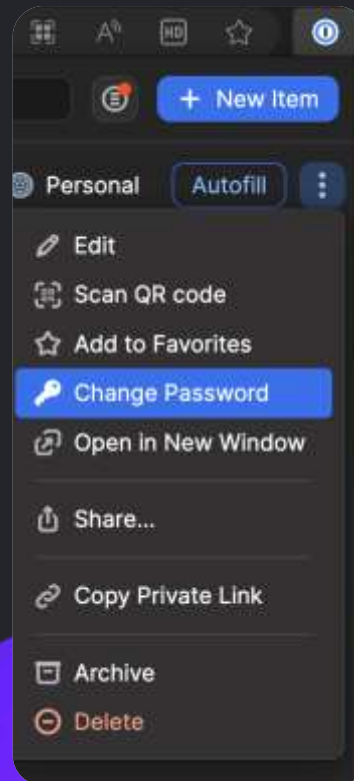
# autocomplete eigindi

- <https://developer.mozilla.org/en-US/docs/Web/HTML/Attributes/autocomplete>
- Lýsir tilgangi innsláttarreita, t.d.
  - current-password
  - new-password
  - one-time-code
- `<input type="password" ... autocomplete="new-password">`



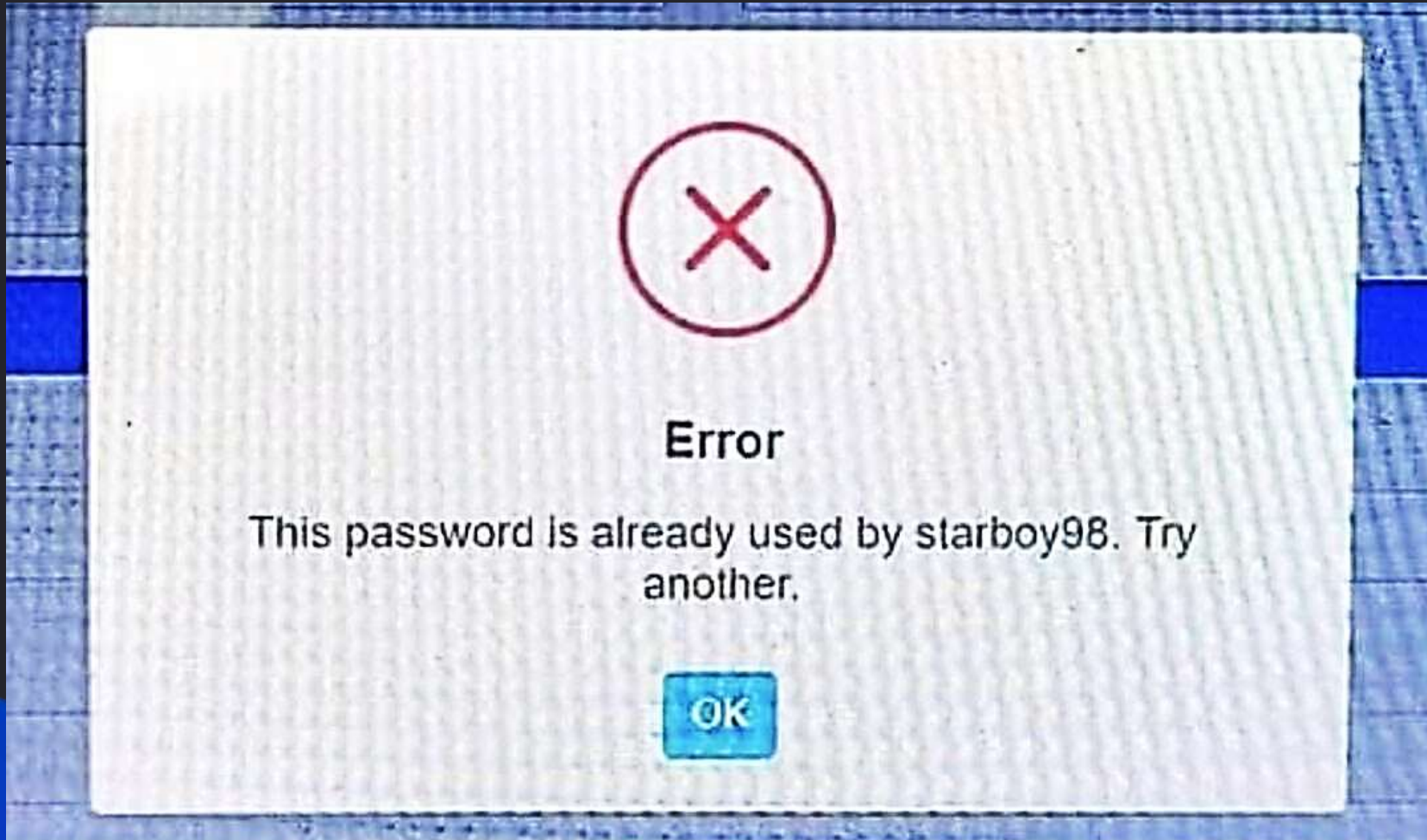
# /.well-known/change-password

- <https://www.w3.org/TR/change-password-url/>
- Vefslóð sem segir lykilorðageymslum hvar notendur geta breytt lykilorðunum.
- Setja upp „redirect“ (HTTP kóði 302, 303 or 307) með Location header á slóðina þar lykilorðum er breytt



# Öll lykilorð ættu að vera einstök!

- Bara ekki útfæra það svona... 🙄



# Takk fyrir!

- Blog: <https://stebet.net>
- Twitter: @stebets
- Email: [stefan@stebet.net](mailto:stefan@stebet.net)