‘;--have i been pwned?

Þetta þarf ekki að vera svona flókið!

LUCINITY

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

LUCINITY

LUCINITY

Lykilorð eru svo “skemmtileg”

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

Flókin lykilorð

password

Flókin lykilorð

Password

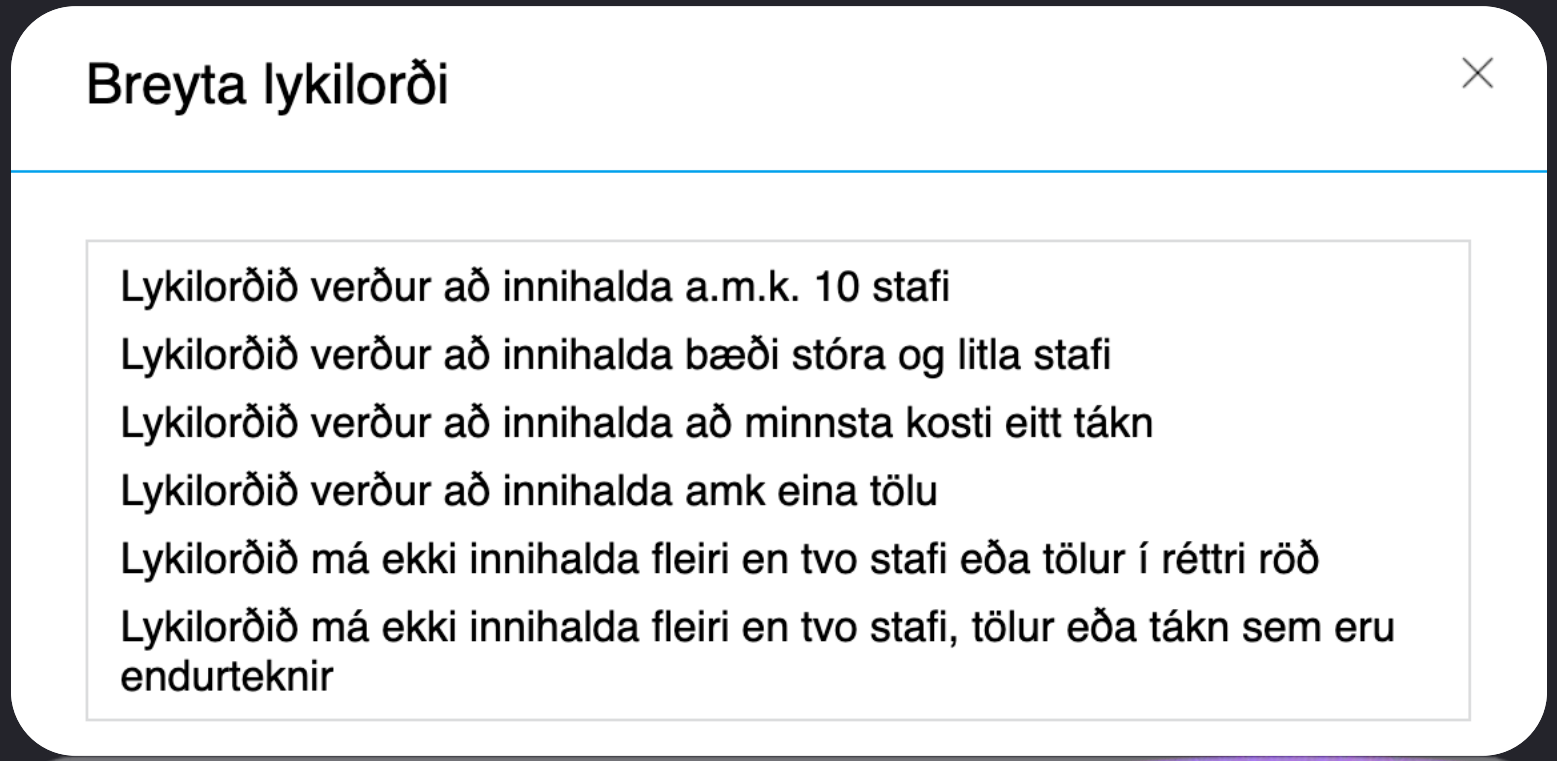
Flókin lykilorð

Password1

Flókin lykilorð

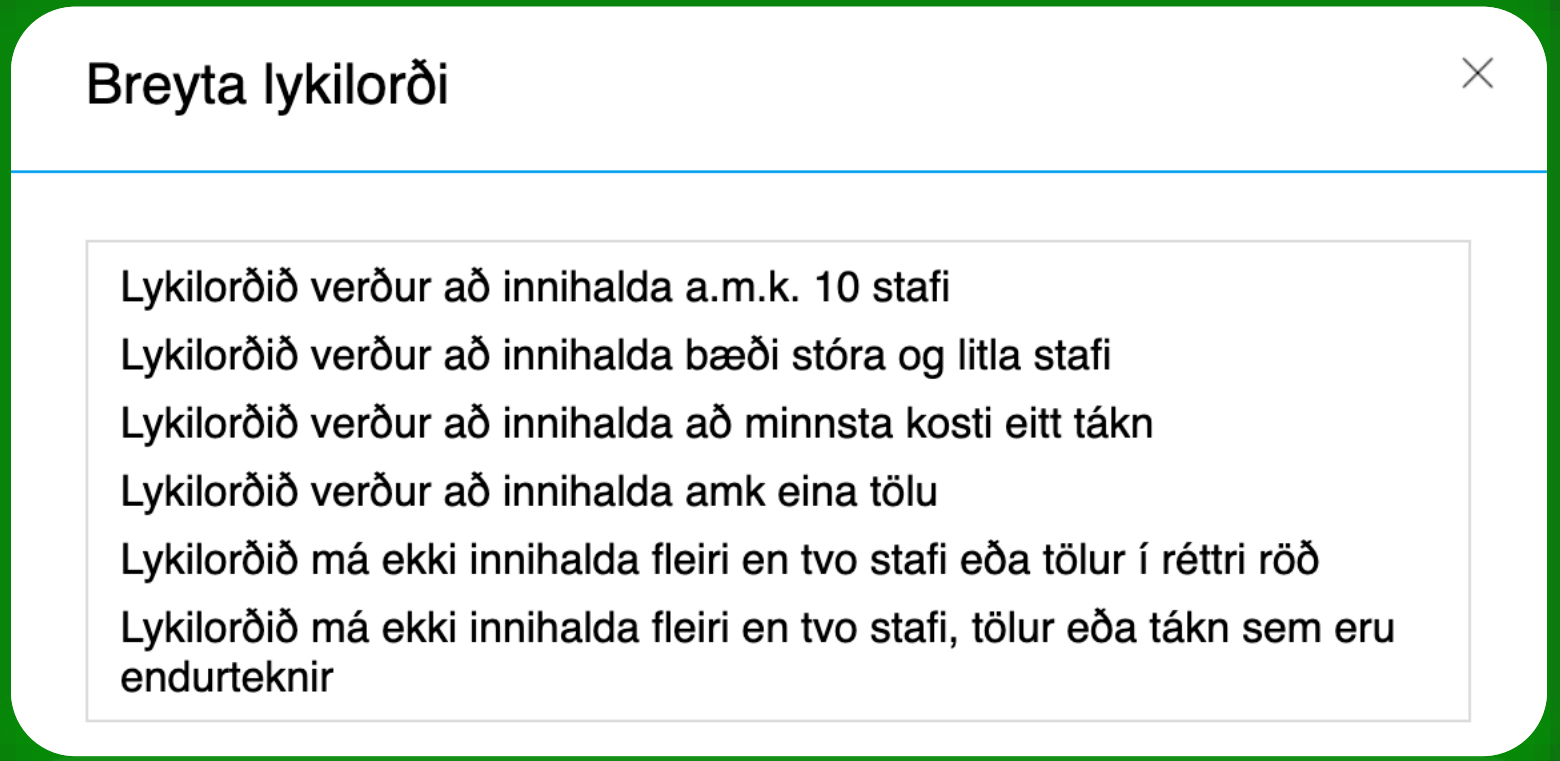
Password1!

Flókin lykilorð



LUCINITY

Flókin lykilorð

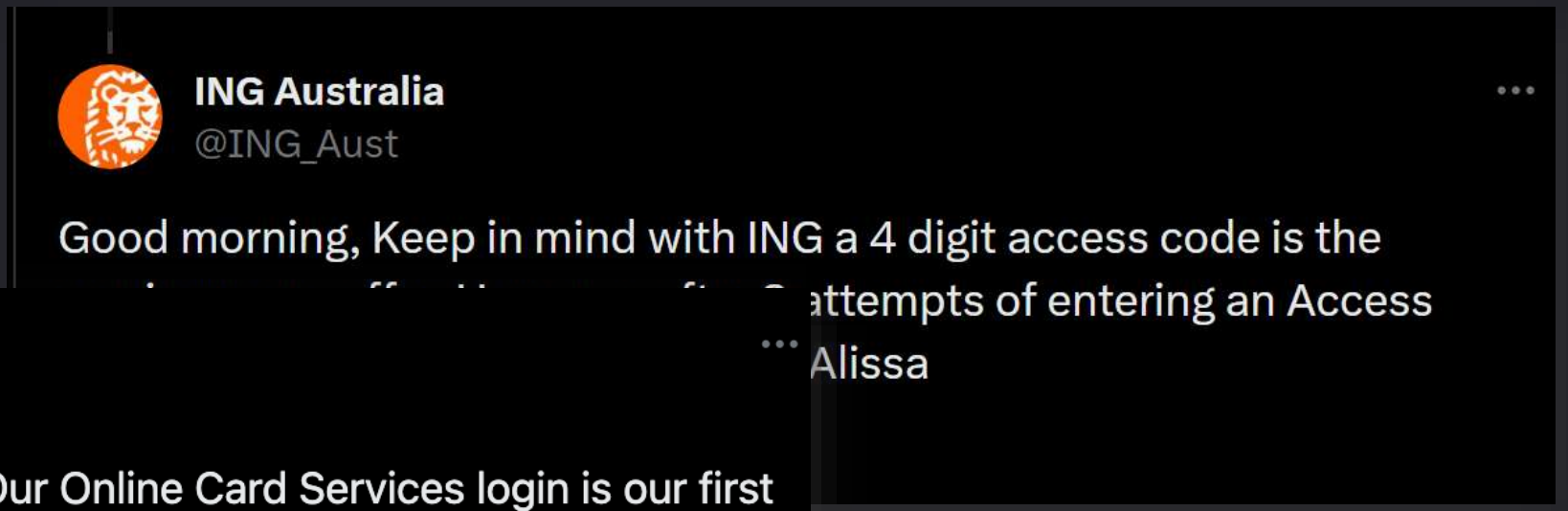


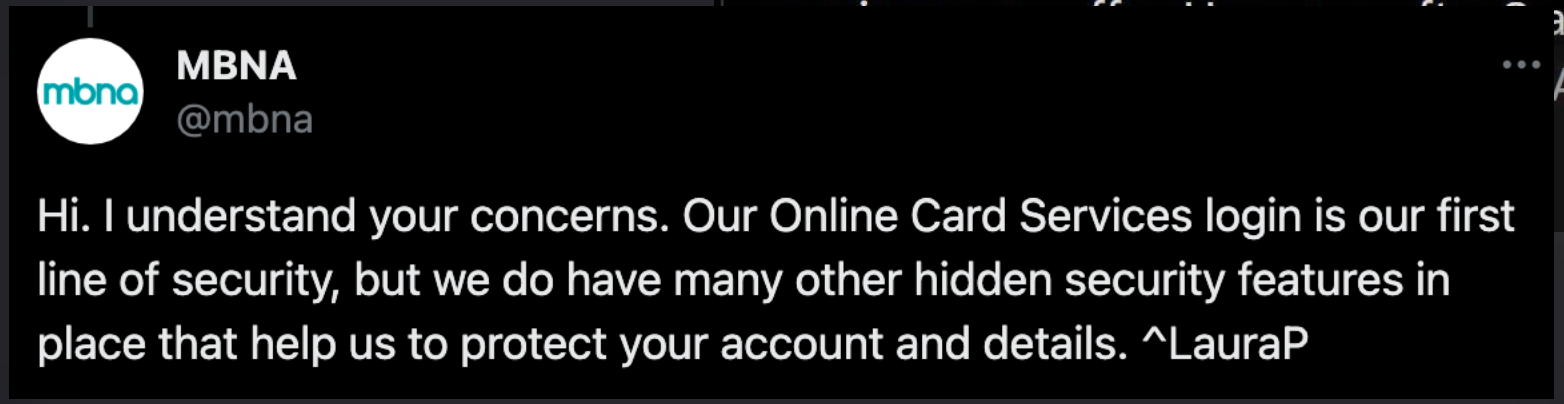
Password1!

LUCINITY


COSSSIP ASSVORD
Creat 0:3321 passwrd !

Réttlætingar





LUCINITY

En er til “rétt” leið?

LUCINITY

Já!

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

LUCINITY

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.”*

LUCINITY

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”*

LUCINITY

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.”***

LUCINITY

Ekki hægt að „pastea“ 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.”*

LUCINITY

Öryggisspurningar

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

Öryggisspurningar

LUCINITY

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 gagnalekum**
- **Auðveldið notendum að nota lykilorðageymslur (Password Manager)**
- **Leiðbeinið!**

LUCINITY

Er lykilorðið í gagnalekum?

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

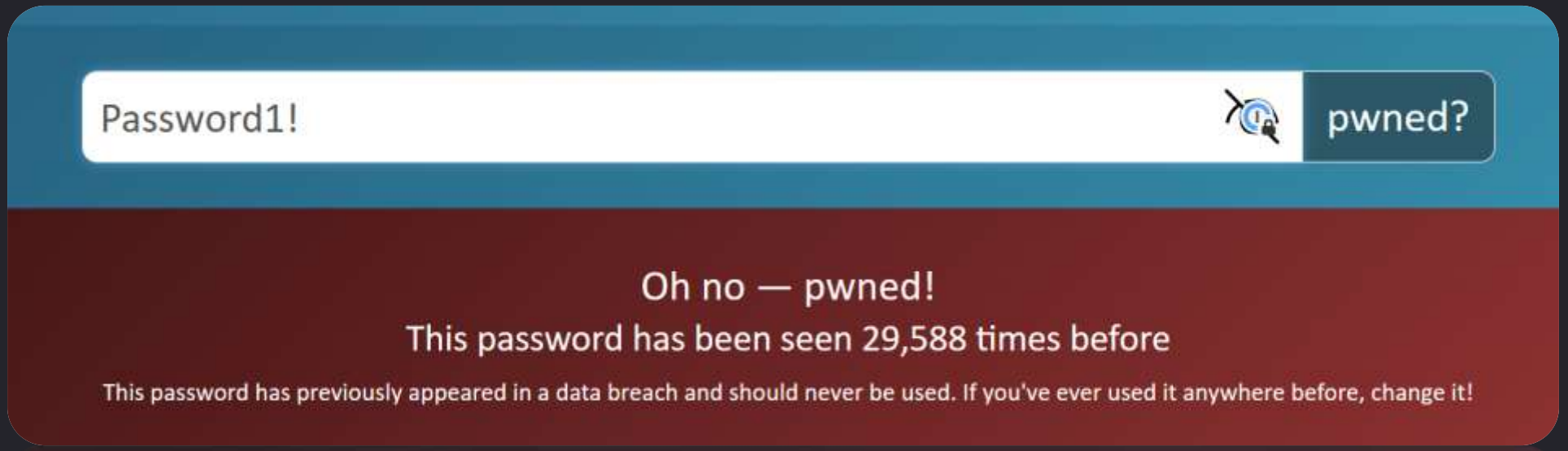
LUCINITY

Pwned Passwords API

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

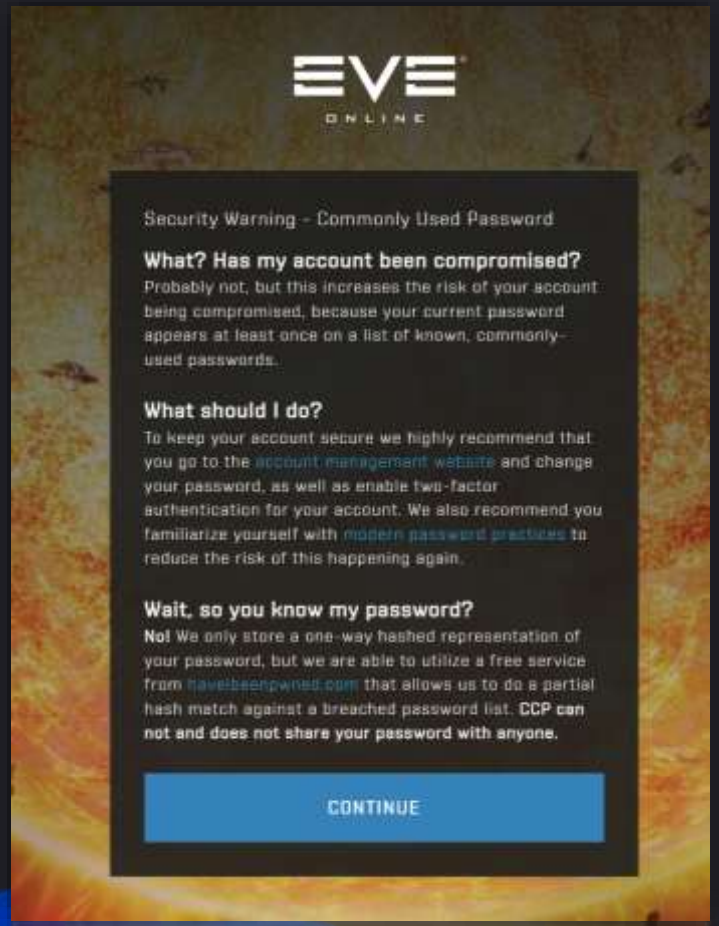
LUCINITY

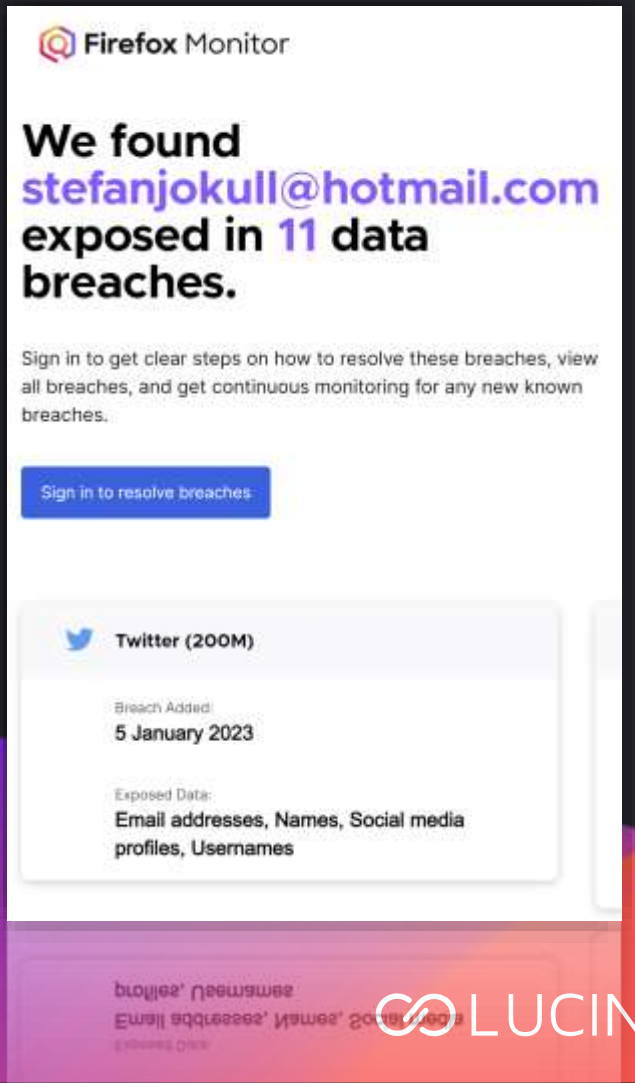
Hversu oft hefur lykilorðið “Password1!” lekið?



LUCINITY

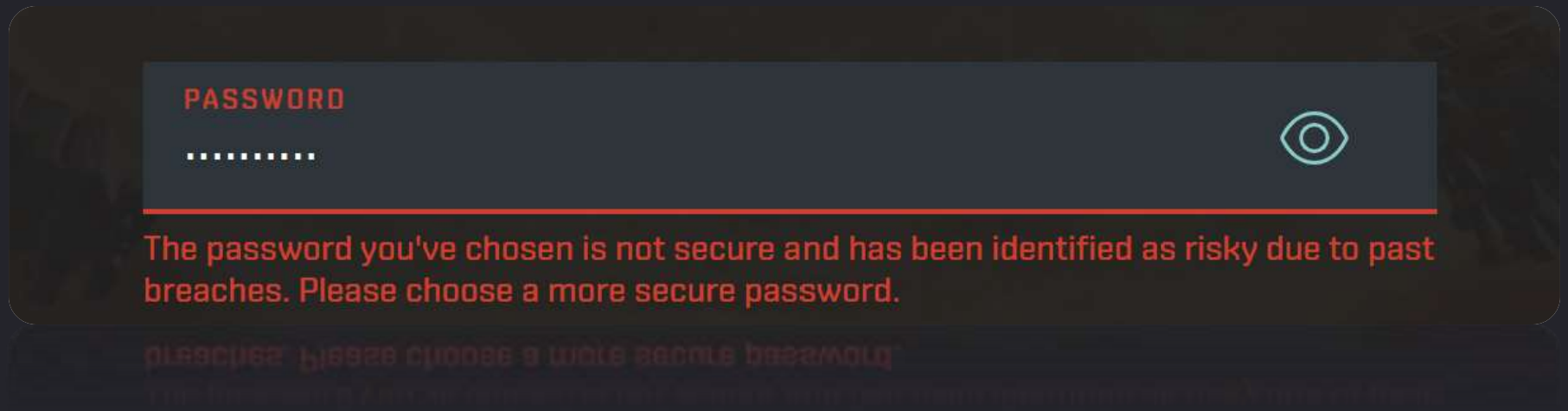
Leiðbeinið – dæmi um notkun á Pwned Passwords





LUCINITY

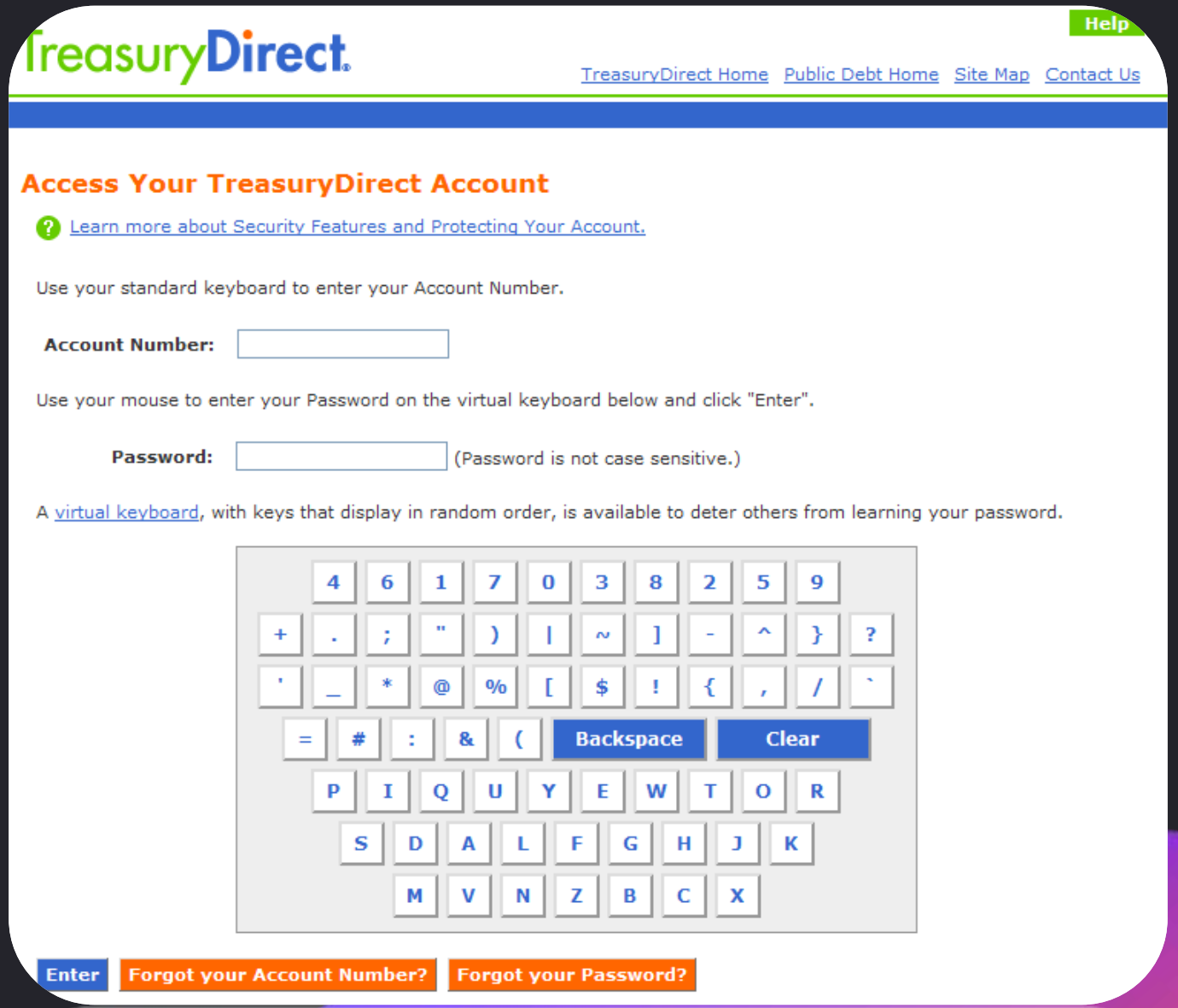
Leiðbeinið – dæmi um notkun á Pwned Passwords



LUCINITY

Ekki þvælast fyrir!

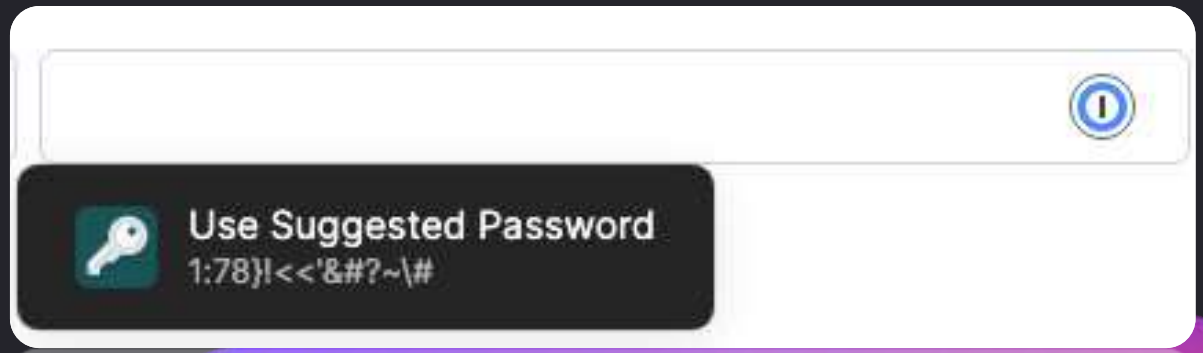
- Leyfið notendum að „pastea“ lykilorð
- Ekki koma í veg fyrir að notendur geti notað lyklaborðið og tólin sín, t.d. með sérstökum “skjályklaborðum“ (on-screen keyboards)


TreasuryDirect
Help
TreasuryDirect Home
Public Debt Home
Site Map
Contact Us
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.
4 6 1 7 0 3 8 2 5 9
+ . ; ") | ~] - ^ } ?
' _ * @ % [$! { , / `
= # : & (Backspace Clear
P I Q U Y E W T O R
S D A L F G H J K
M V N Z B C X
Enter
Forgot your Account Number?
Forgot your Password?

LUCINITY

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;



LUCINITY

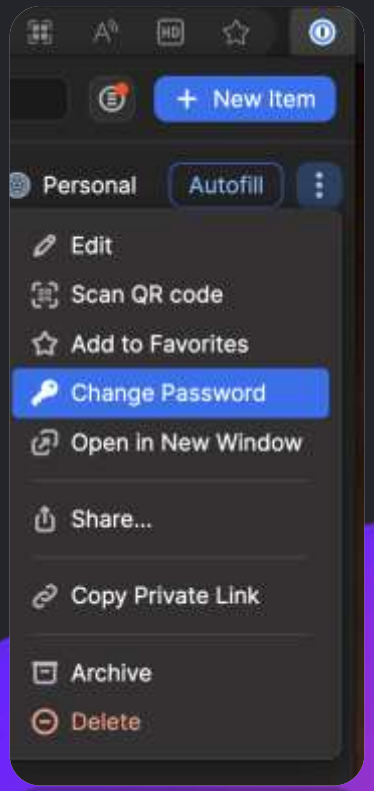
autocomplete eigindi

- 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">**

LUCINITY

/.well-known/change-password

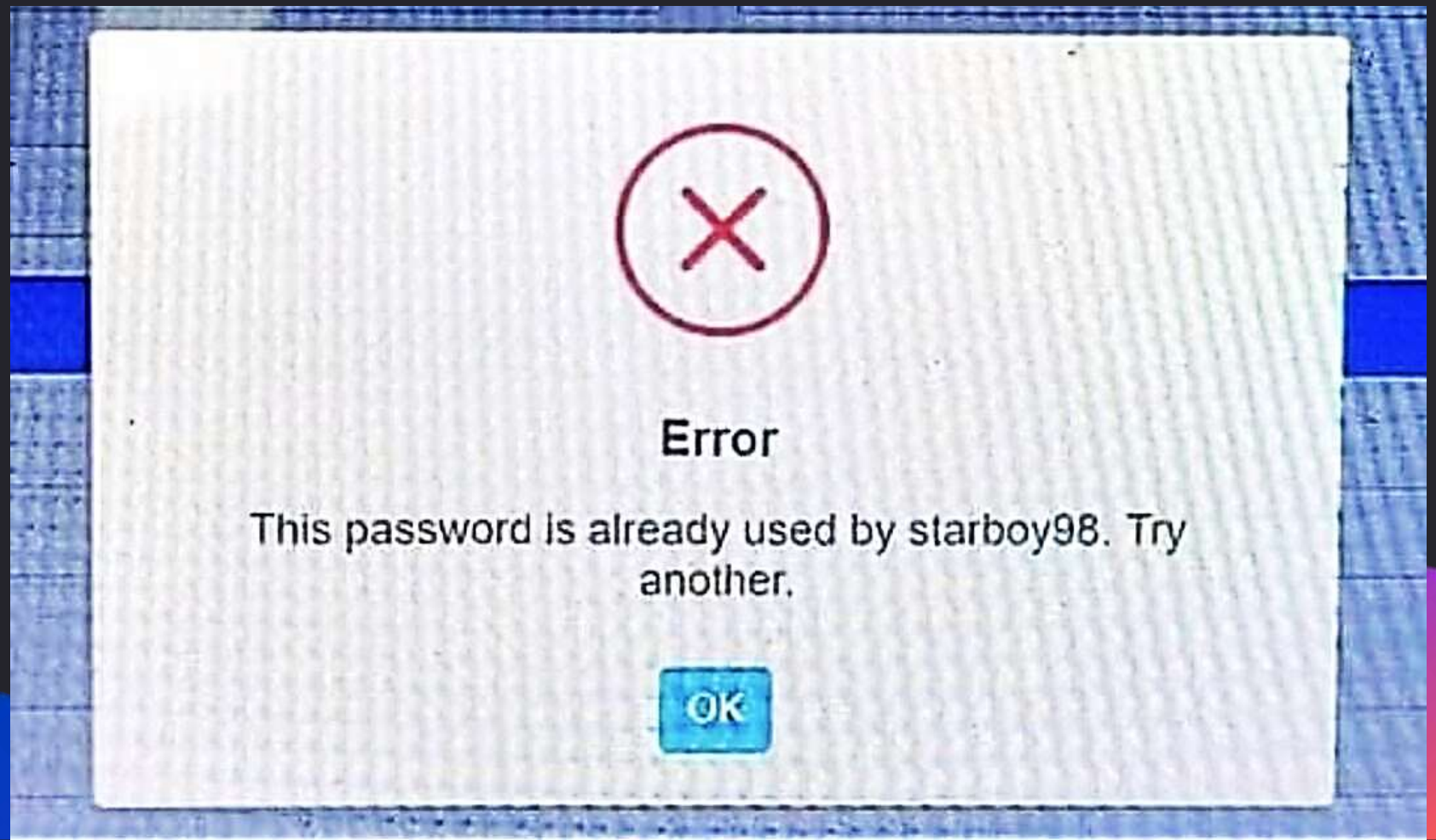
- https://www.w3.org/TR/change-password-url/
- Vefslóð sem segir lykilorðageymslum hvar notendur geta breytt lykilorðunum.
- Setja upp „redirect“ (HTTP kóði 302, 303 or 307) með Location header á slóðina þar lykilorðum er breytt



LUCINITY

Öll lykilorð ættu að vera einstök!

- Bara ekki útfæra það svona… 🥹



LUCINITY

Takk fyrir!

- Blog: https://stebet.net
- Twitter: @stebets
- Email: stefan@stebet.net