08. Authentication Part 3 & Access Control

Blase Ur and David Cash
January 23rd, 2023
CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

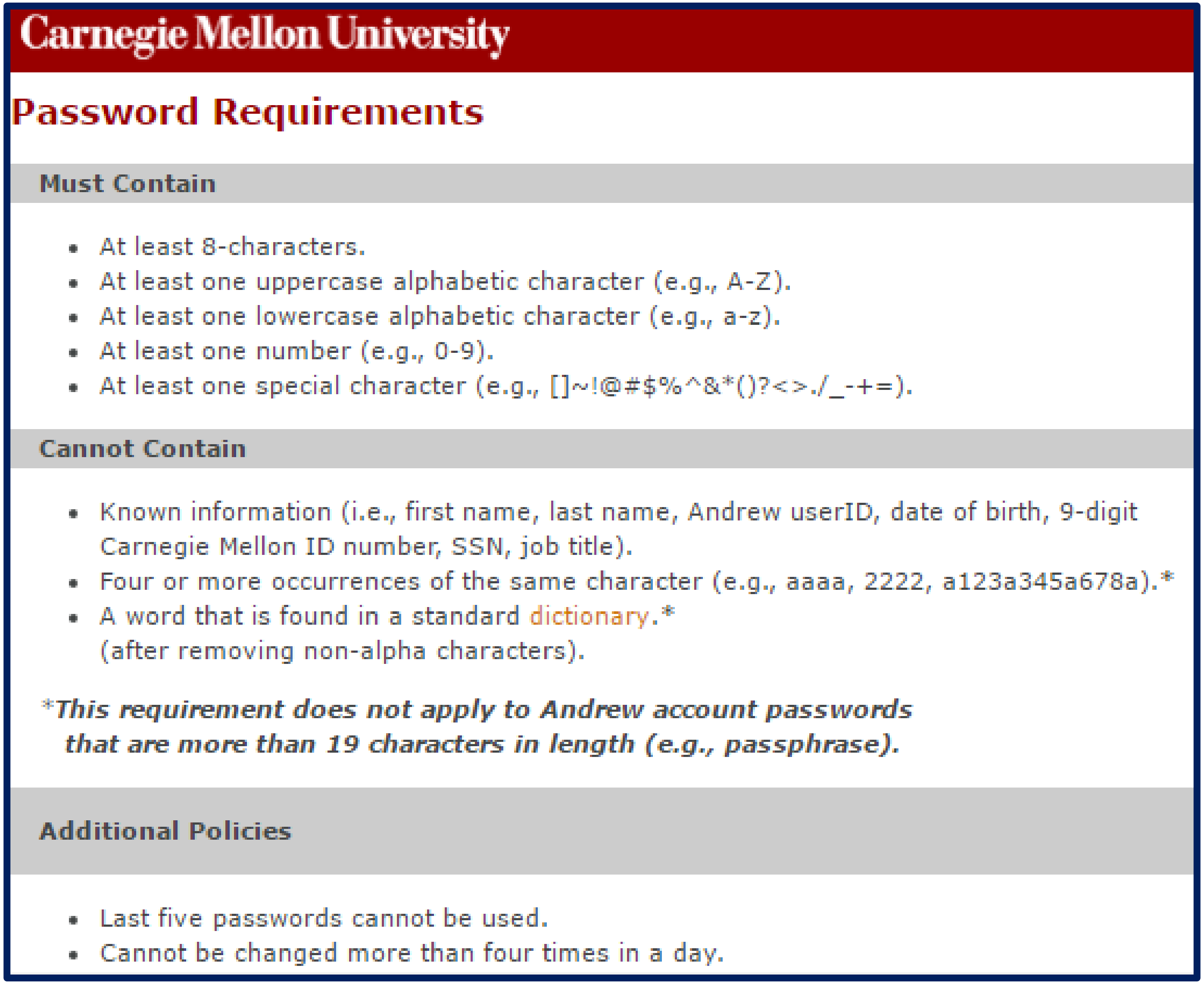
User-Centered Security

Some Ways to Understand Users

- Retrospective analysis of user-created password breaches
- Large-scale online studies
- Examine real passwords with permission
- Qualitative studies

How Do We Help Users Make Better Passwords?

Problem 1: Bad Advice



Carnegie Mellon University

Password Requirements

Must Contain

- At least 8-characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., []~!@#$%^&*()?<>./_-+=).

Cannot Contain

- Known information (i.e., first name, last name, Andrew userID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).
- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*
- A word that is found in a standard dictionary.*
  (after removing non-alpha characters).

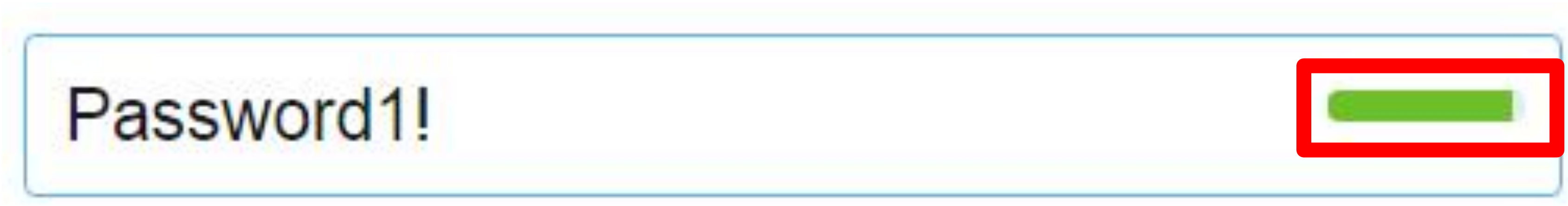
****This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).***

Additional Policies

- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.

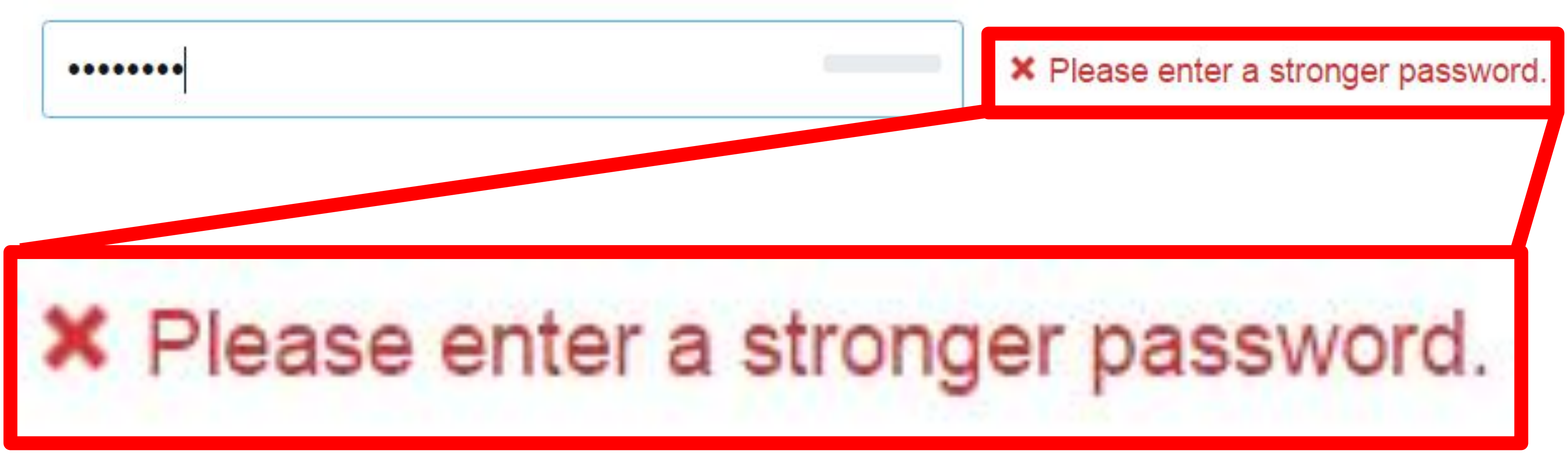
Problem 2: Inaccurate Feedback

twitter



Password1!

Problem 3: Unhelpful Feedback



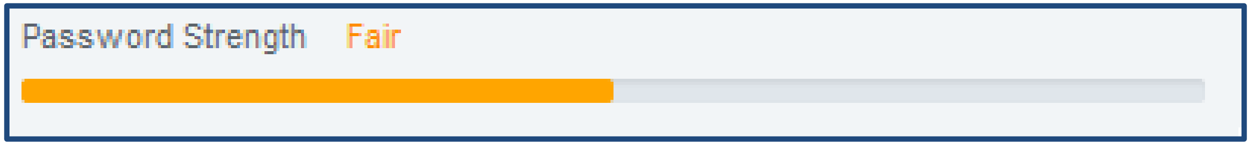
••••••••

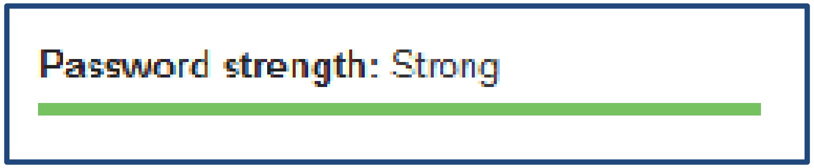
✖ Please enter a stronger password.

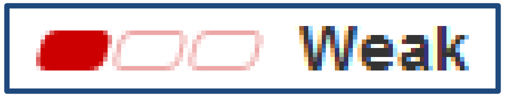
✖ Please enter a stronger password.

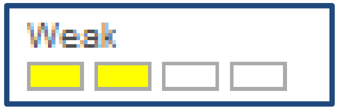
Proactive Strength Checking

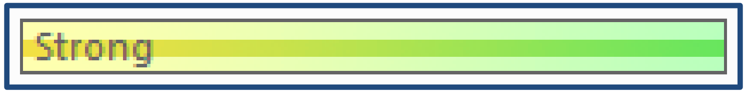
- Initial idea: provide feedback
- In practice: complexities regarding what to model, and how to do so efficiently

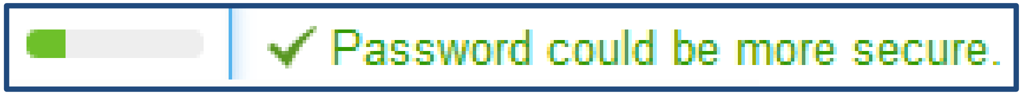

Password Strength Fair


Password strength: Strong


Weak


Weak


Strong

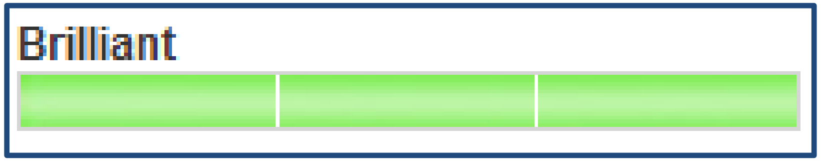

✓ Password could be more secure.

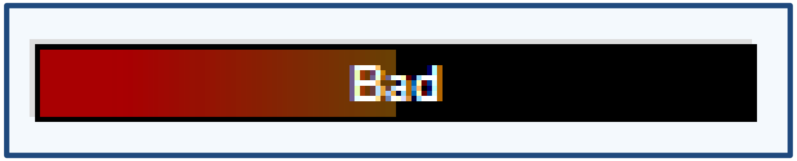
Meters’ Security & Usability Impact

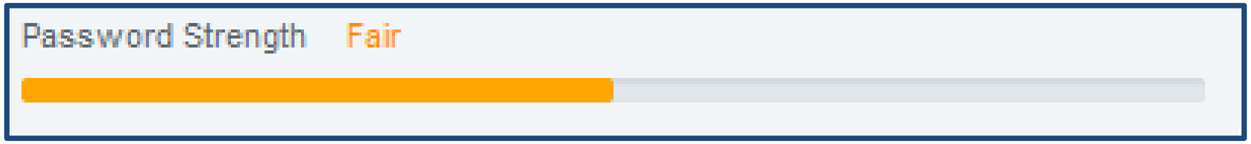
Password
WEAK
STRONG

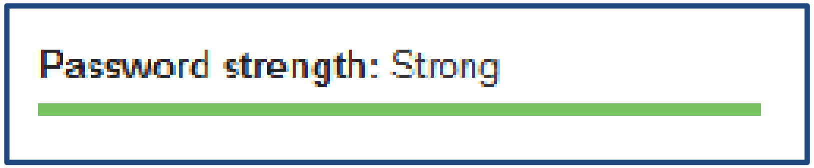
Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proc. USENIX Security Symposium*, 2012.

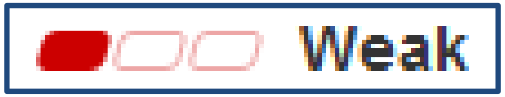
Meters Are Ubiquitous

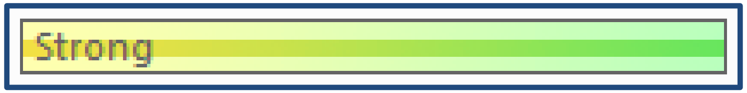


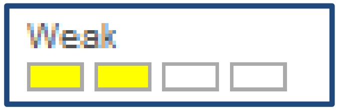


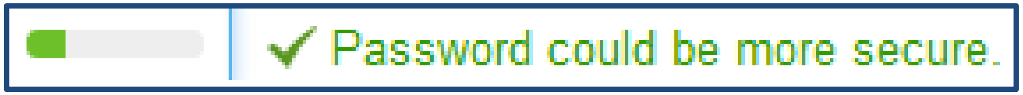



Password strength: Strong





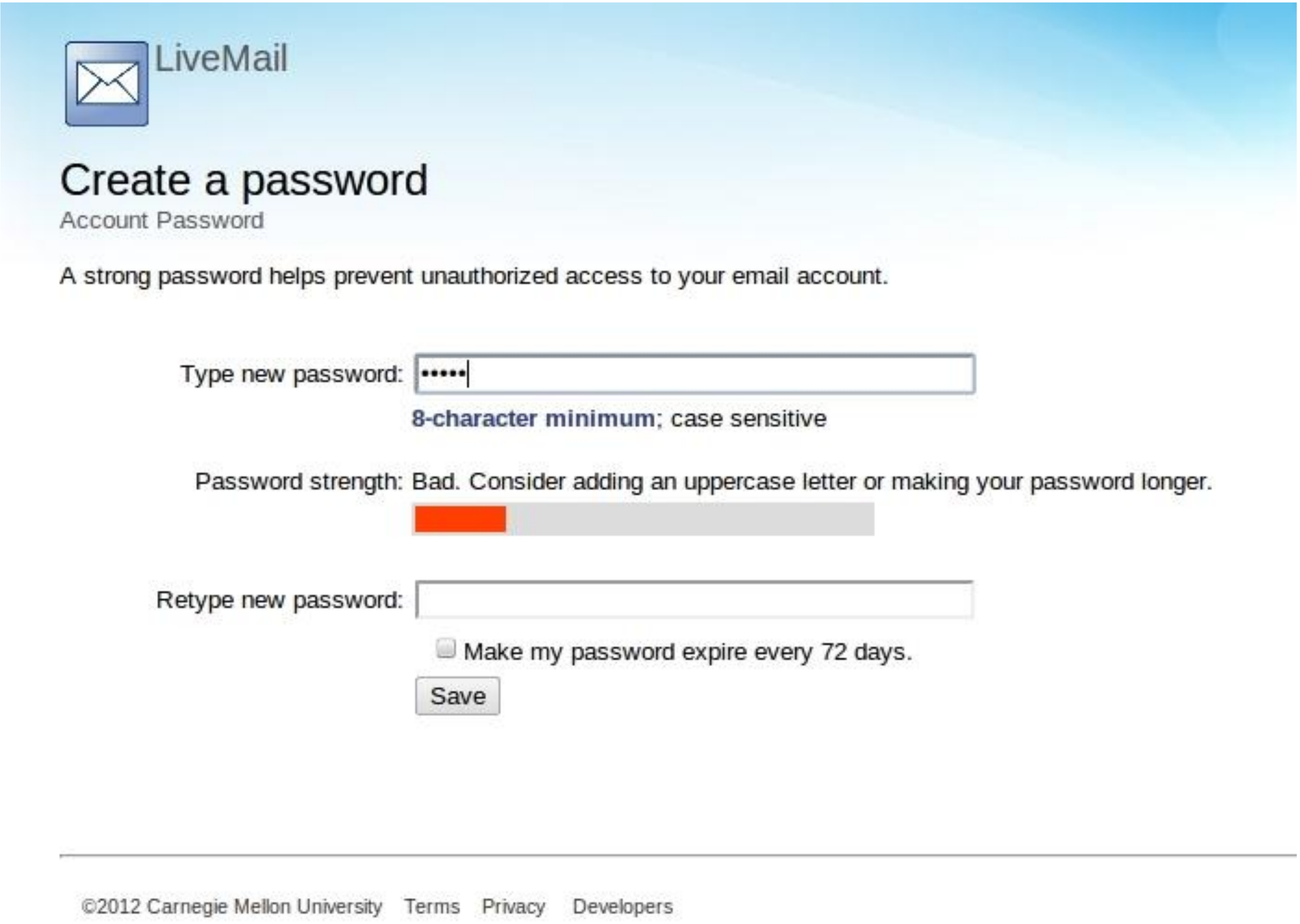



✓ Password could be more secure.

Test Meters' Impact

- How do meters impact password security?
- How do meters impact usability?
  - Memorability
  - User sentiment
  - Timing
- What meter features matter?
- 2,931-participant online study

Baseline Password Meter



Create a password

Account Password

A strong password helps prevent unauthorized access to your email account.

Type new password: •••••

8-character minimum; case sensitive

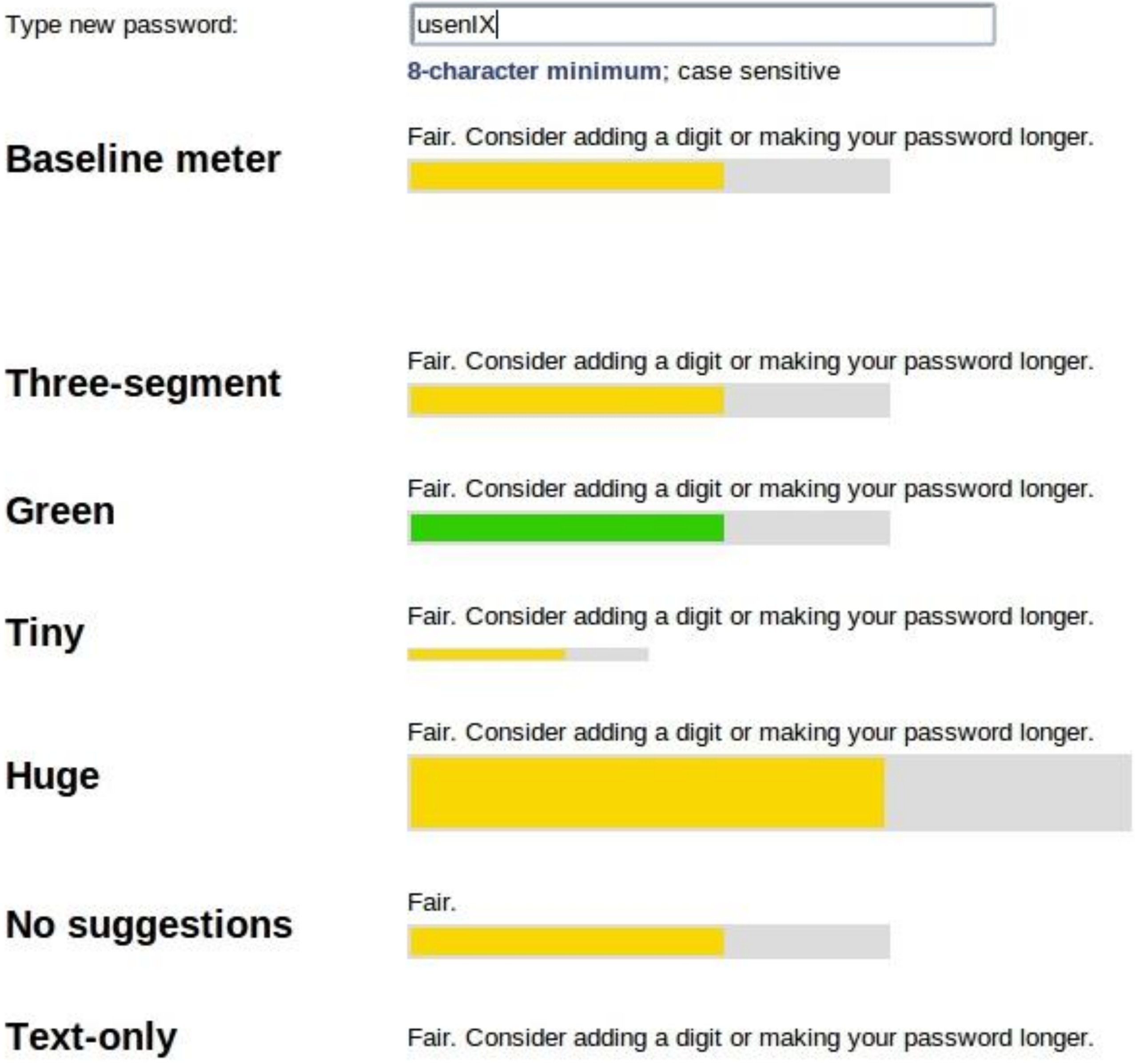
Password strength: Bad. Consider adding an uppercase letter or making your password longer.

Retype new password:

□ Make my password expire every 72 days.

©2012 Carnegie Mellon University Terms Privacy Developers

Visual Differences



Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Three-segment

Fair. Consider adding a digit or making your password longer.

Green

Fair. Consider adding a digit or making your password longer.

Tiny

Fair. Consider adding a digit or making your password longer.

Huge

Fair. Consider adding a digit or making your password longer.

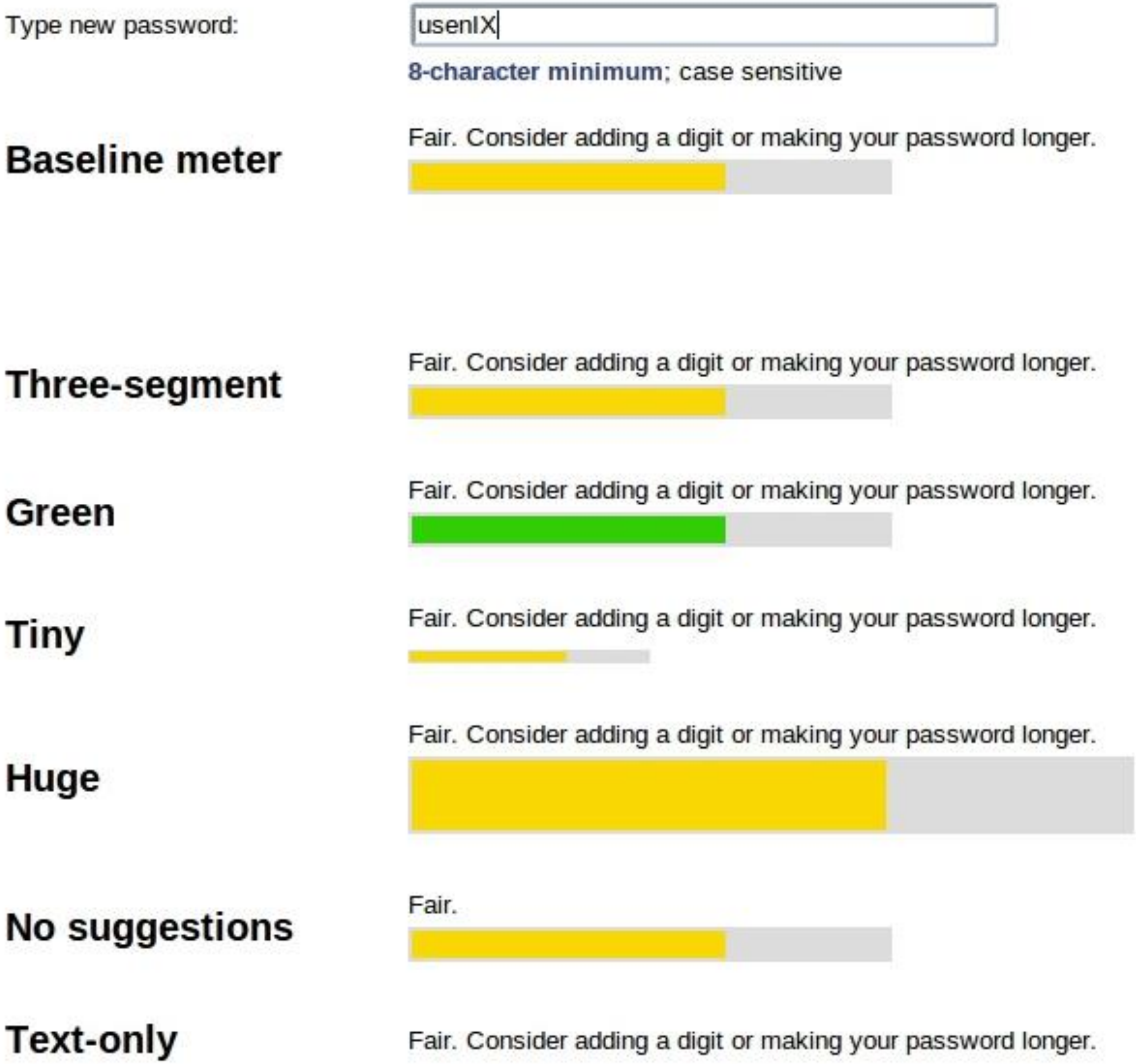
No suggestions

Fair.

Text-only

Fair. Consider adding a digit or making your password longer.

Visual Differences



Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Three-segment

Fair. Consider adding a digit or making your password longer.

Green

Fair. Consider adding a digit or making your password longer.

Tiny

Fair. Consider adding a digit or making your password longer.

Huge

Fair. Consider adding a digit or making your password longer.

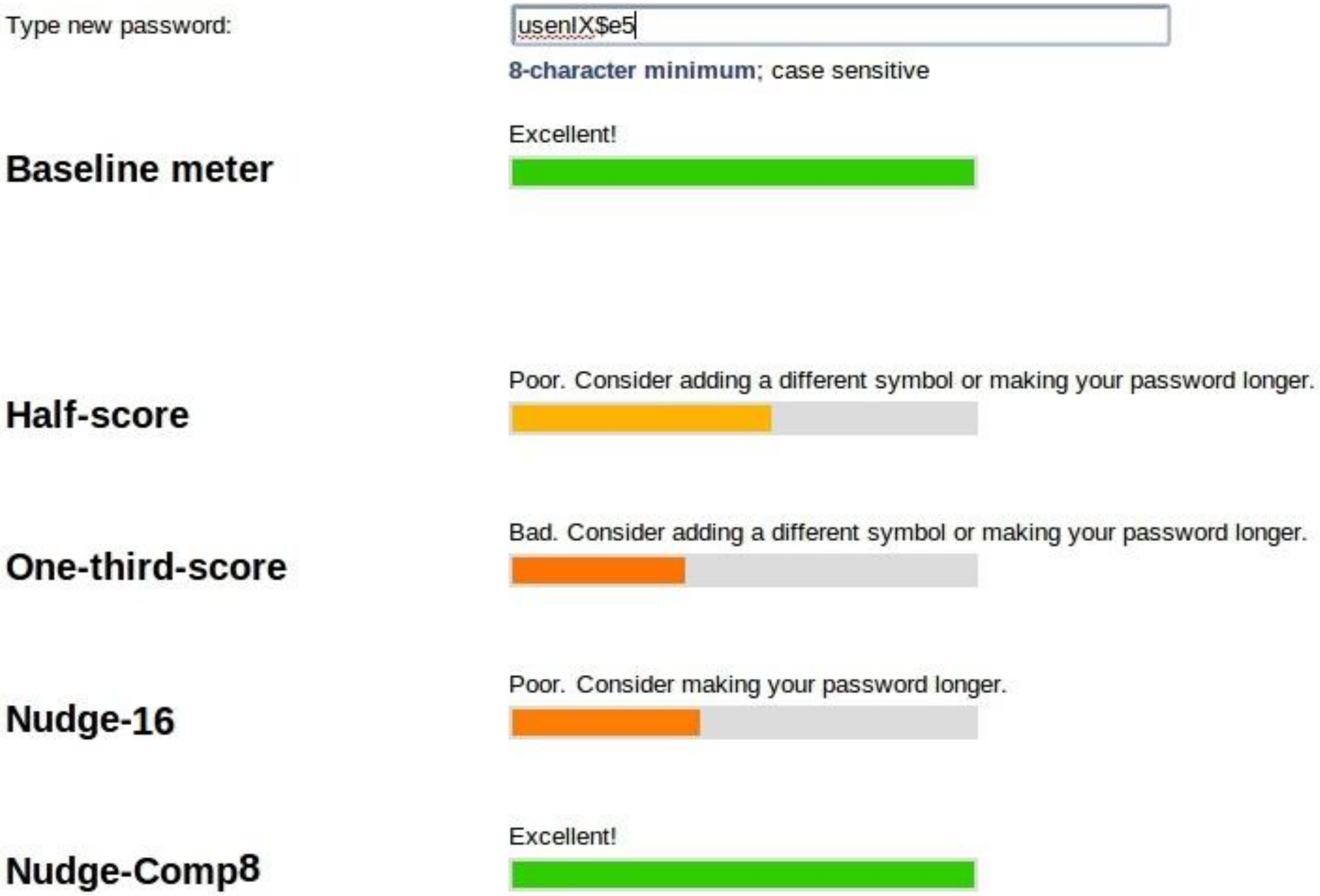
No suggestions

Fair.

Text-only

Fair. Consider adding a digit or making your password longer.

Scoring Differences



Type new password: usenIX$e5

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Poor. Consider adding a different symbol or making your password longer.

One-third-score

Bad. Consider adding a different symbol or making your password longer.

Nudge-16

Poor. Consider making your password longer.

Nudge-Comp8

Excellent!

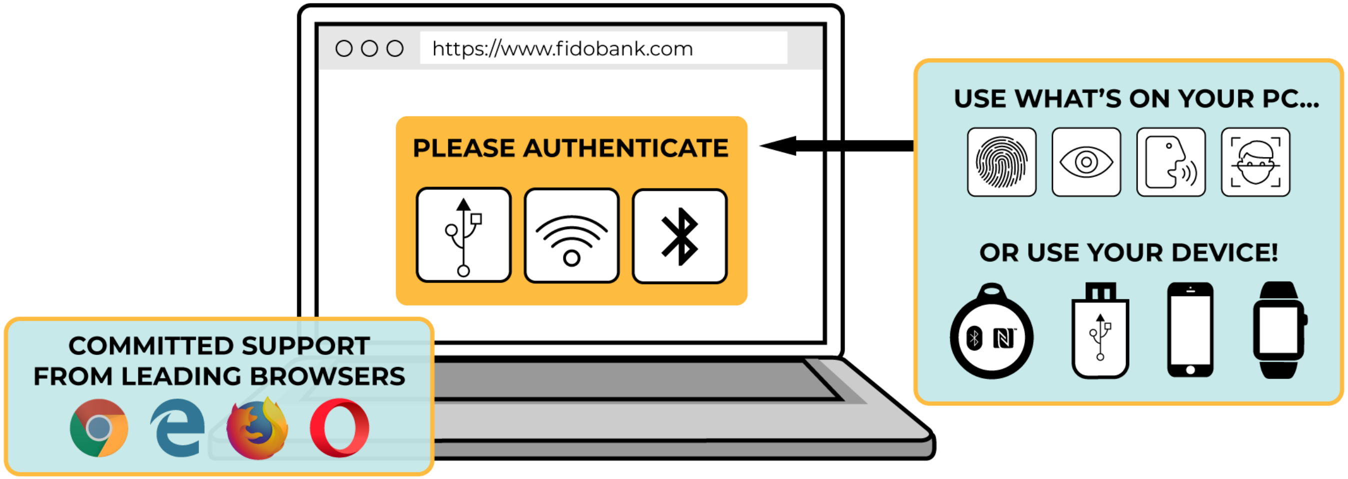
Key Results

- Stringent meters with visual bars increased resistance to guessing
- Visual differences did not significantly impact resistance to guessing
- No significant impact on memorability

Authentication in Practice: Moving Towards A Passwordless World?

Case Study: WebAuthn

FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS



https://www.fidobank.com

PLEASE AUTHENTICATE

USE WHAT'S ON YOUR PC...

OR USE YOUR DEVICE!

COMMITTED SUPPORT FROM LEADING BROWSERS

FIDO AUTHENTICATION: THE NEW GOLD STANDARD

Protects against phishing, man-in-the-middle and attacks using stolen credentials

Log in with a single gesture – HASSLE FREE!

aetna

Bank of America

Dropbox

ebay

facebook

Google

docomo

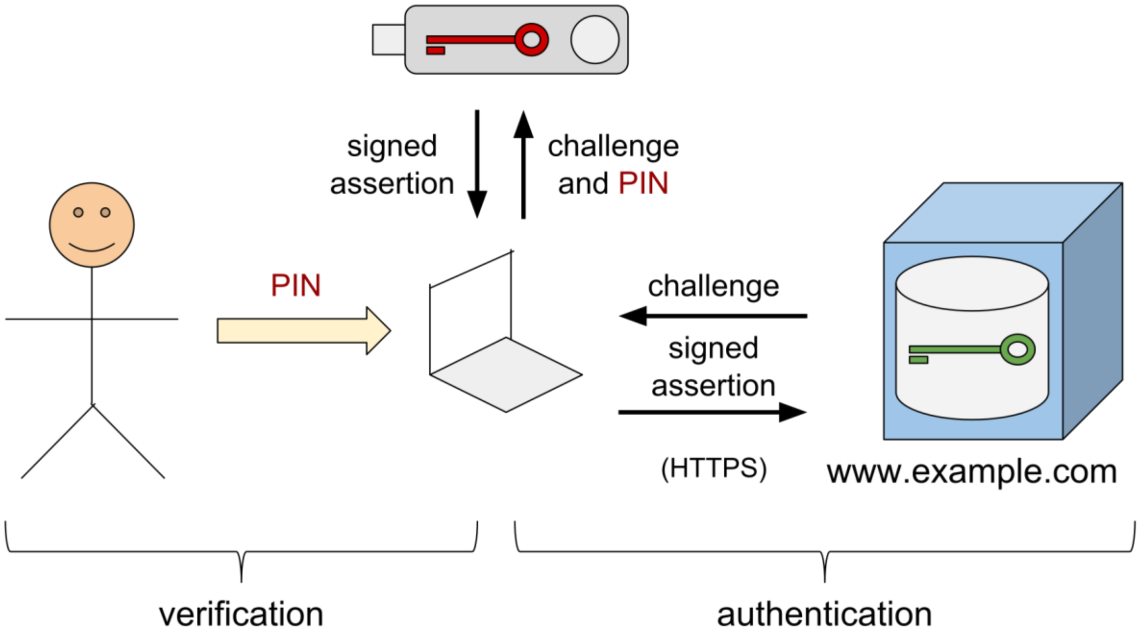
PayPal

salesforce

Already supported in market by top online services

Case Study: WebAuthn

- Created under the FIDO2 project, now a W3C standard
- Goal: Authenticate on web using public-key crypto
- Implemented in specialized hardware OR in software using a TPM/TEE



Case Study: WebAuthn

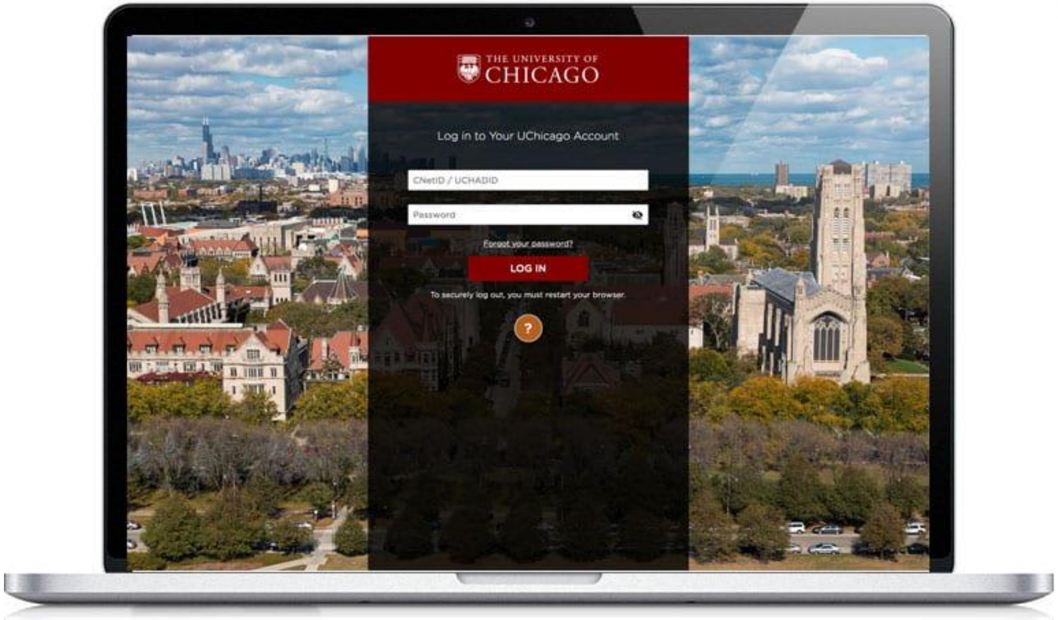
User interaction: Push a button on a key, type a PIN into the device, present biometric (fingerprint) to hardware reader

Authentication in Practice: Password Add-Ons / Alternatives

Single Sign-On

Login with Facebook

OpenID®



THE UNIVERSITY OF CHICAGO

Log in to Your UChicago Account

CNetID / UCHADID

Password

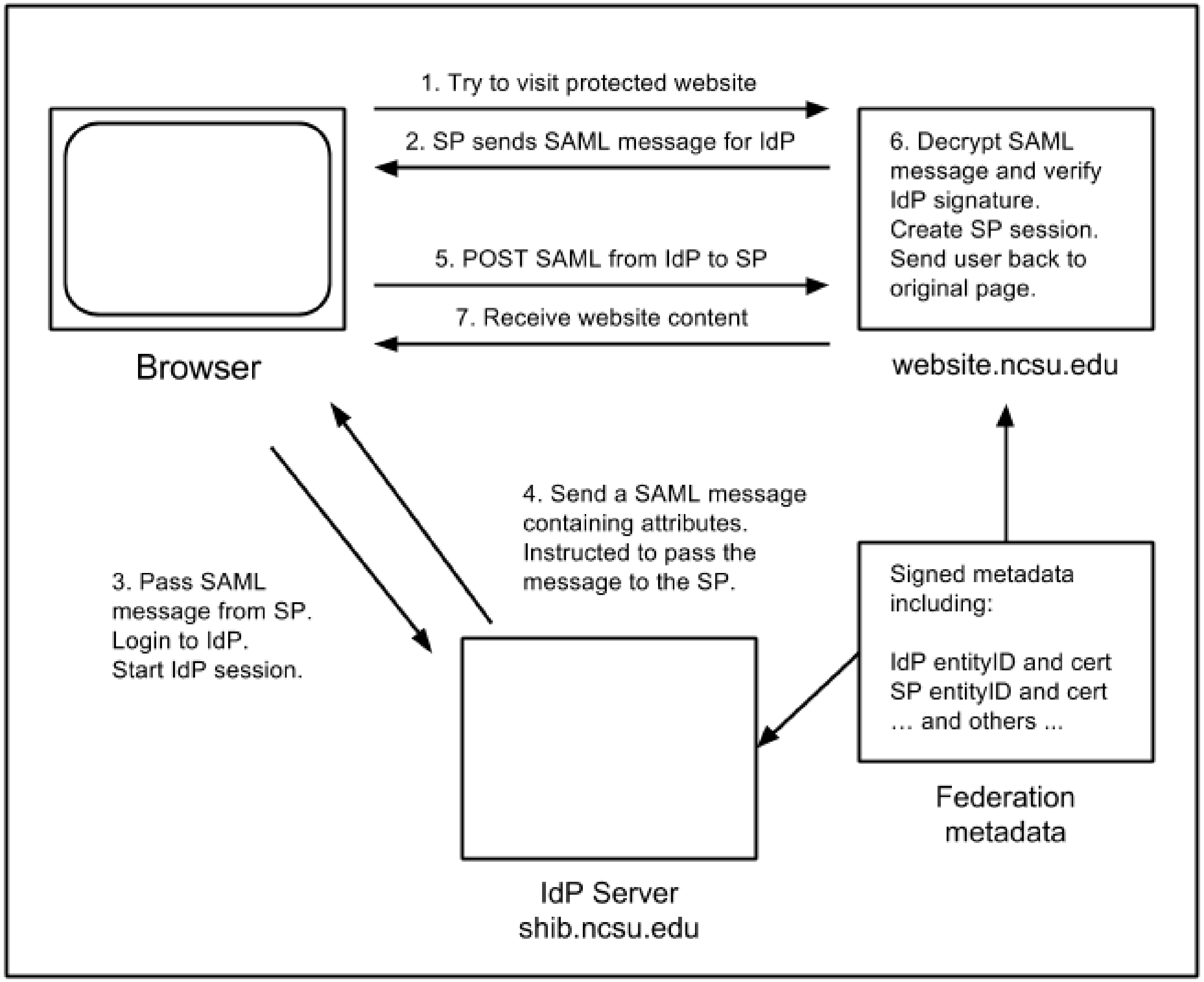
Forgot your password?

LOG IN

To securely log out, you must restart your browser.

?

Single Sign-On: Shibboleth

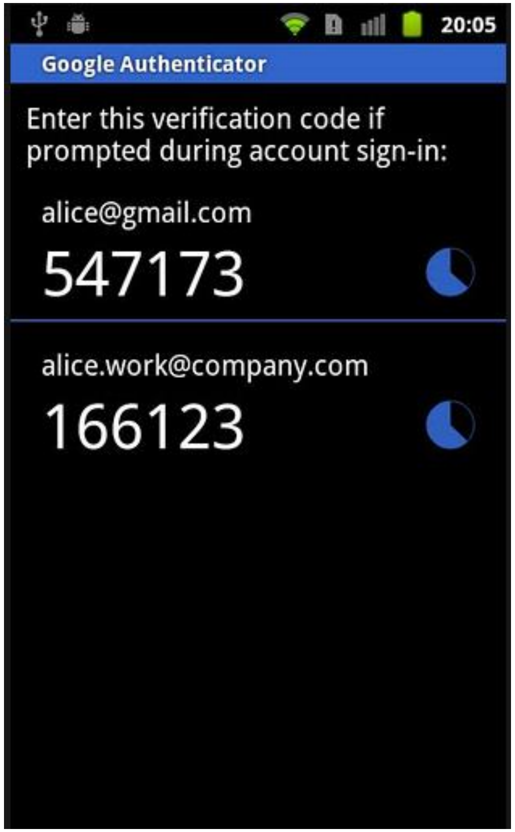


1. Try to visit protected website
2. SP sends SAML message for IdP
5. POST SAML from IdP to SP
7. Receive website content
Browser
6. Decrypt SAML message and verify IdP signature. Create SP session. Send user back to original page.
website.ncsu.edu
3. Pass SAML message from SP. Login to IdP. Start IdP session.
4. Send a SAML message containing attributes. Instructed to pass the message to the SP.
Signed metadata including:
IdP entityID and cert
SP entityID and cert
... and others ...
Federation metadata
IdP Server
shib.ncsu.edu

Diagram from https://docs.shib.ncsu.edu/docs/shibworks.html

For a good (long) explanation, see: https://www.switch.ch/aai/demo/

Two-Factor Auth

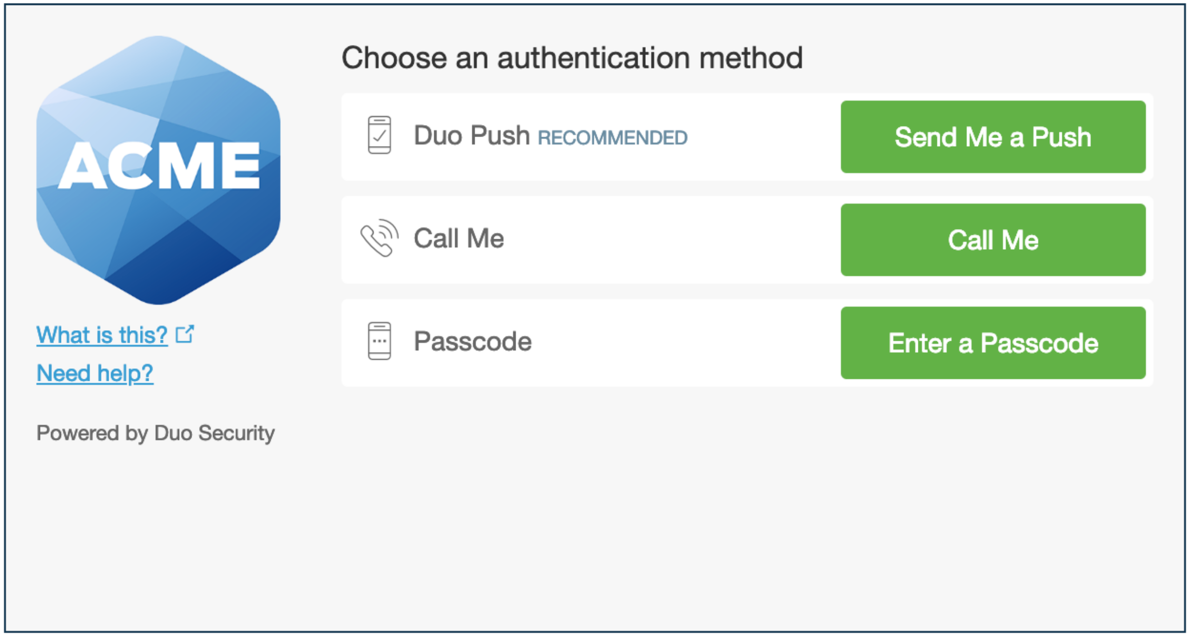


Google Authenticator

Enter this verification code if prompted during account sign-in:

alice@gmail.com
547173

alice.work@company.com
166123



Choose an authentication method

Duo Push RECOMMENDED

Call Me

Passcode

Powered by Duo Security

Physical Tokens / Smart Cards

- Codes based on a cryptographic key
  - Token manufacturer also knows the key
- What if there is a breach?

Authentication in Practice:
I Forgot My Password

Resetting Accounts

- I forgot my password!
- Send an email?
- Security questions?
- In-person verification?
- Other steps?
- (No backup)

Authentication in Practice: Password Managers

Password Managers

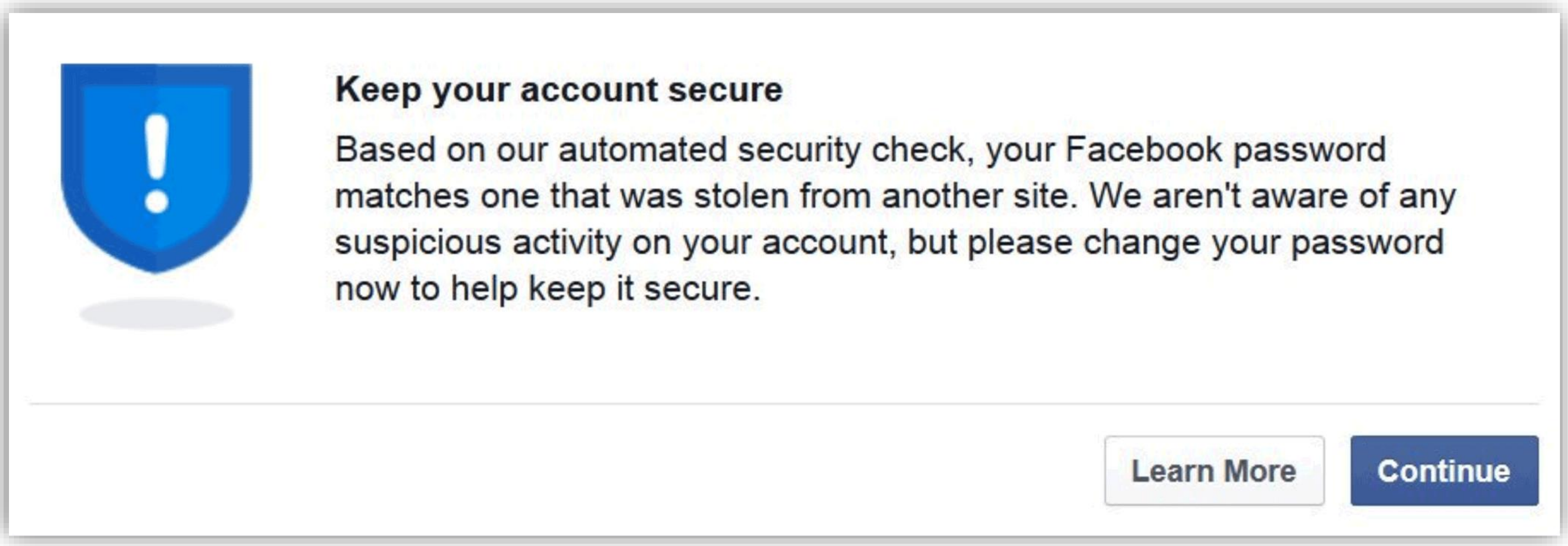
- Trust all passwords to a single master password (still a good idea in most cases)
  - – Also trust software
  - – Centralized vs. decentralized architectures

LastPass****

1Password

Authentication in Practice: Password Reuse ☹

Password Reuse-Based Attacks



Keep your account secure

Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren't aware of any suspicious activity on your account, but please change your password now to help keep it secure.

Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur. "What was that site doing with my Facebook Password?" Designing Password-Reuse Notifications. In *Proc. CCS*, 2018.

People Reuse Passwords

Booking.com
reddit
淘宝网
Taobao.com
American Airlines
facebook
Adobe
ebay
Microsoft
slack
Baidu 百度
airbnb
YouTube
SONY
PayPal
WELLS FARGO
1&1
Dropbox
twitter
Spotify
Google

R0cky!14

R0cky!17

R0cky!17

123456

Rocky!16

R0ckyStar

R0ckyBox

R0cky!17

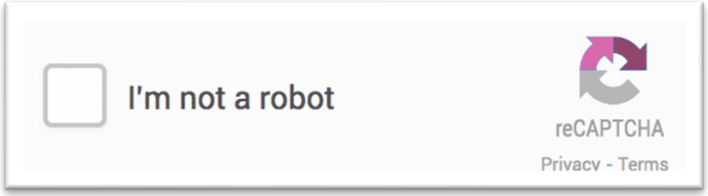
R0cky!17

AcmeCo

Memory-Hard Hash Function ✓

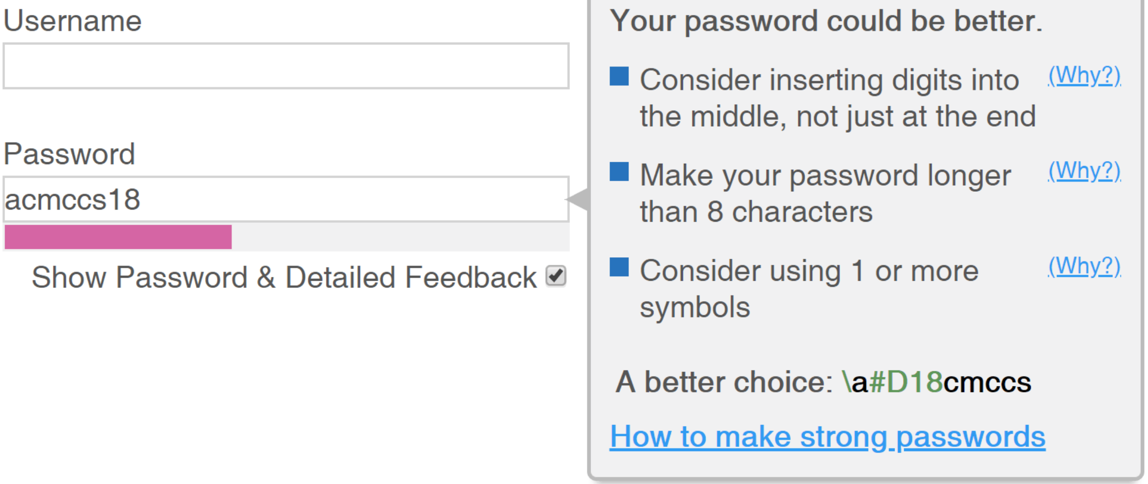
Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

Rate-Limiting Guessing ✓



□ I'm not a robot

Password Strength Meter ✓



Username

Password

acmccs18

Show Password & Detailed Feedback ☑

Your password could be better.

- Consider inserting digits into the middle, not just at the end (Why?)
- Make your password longer than 8 characters (Why?)
- Consider using 1 or more symbols (Why?)

A better choice: \a#D18cmccs

How to make strong passwords

AcmeCo

Email
…
jim@mail.com
…

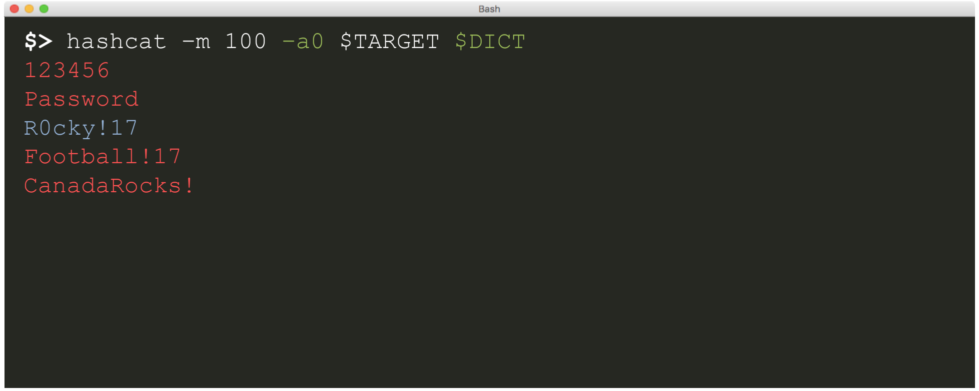
LinkedIn

Email
jane@aol.com
jessey@gmx.net
jenny@gmail.com
jim@mail.com
john@hotmail.com
…

LinkedIn

Email	SHA-1 Hash of Password
jane@aol.com	7c4a8d09ca3762af61e595209
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	7c222fb2927d828af22f59213
jim@mail.com	ba93664a90285b9ff18a7a081
john@hotmail.com	b1b3773a05c0ed0176787a4f1
...	...

Crack All The Things!



```
$> hashcat -m 100 -a0 $TARGET $DICT
123456
Password
R0cky!17
Football!17
CanadaRocks!
```

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

Dead On Arrival

AcmeCo

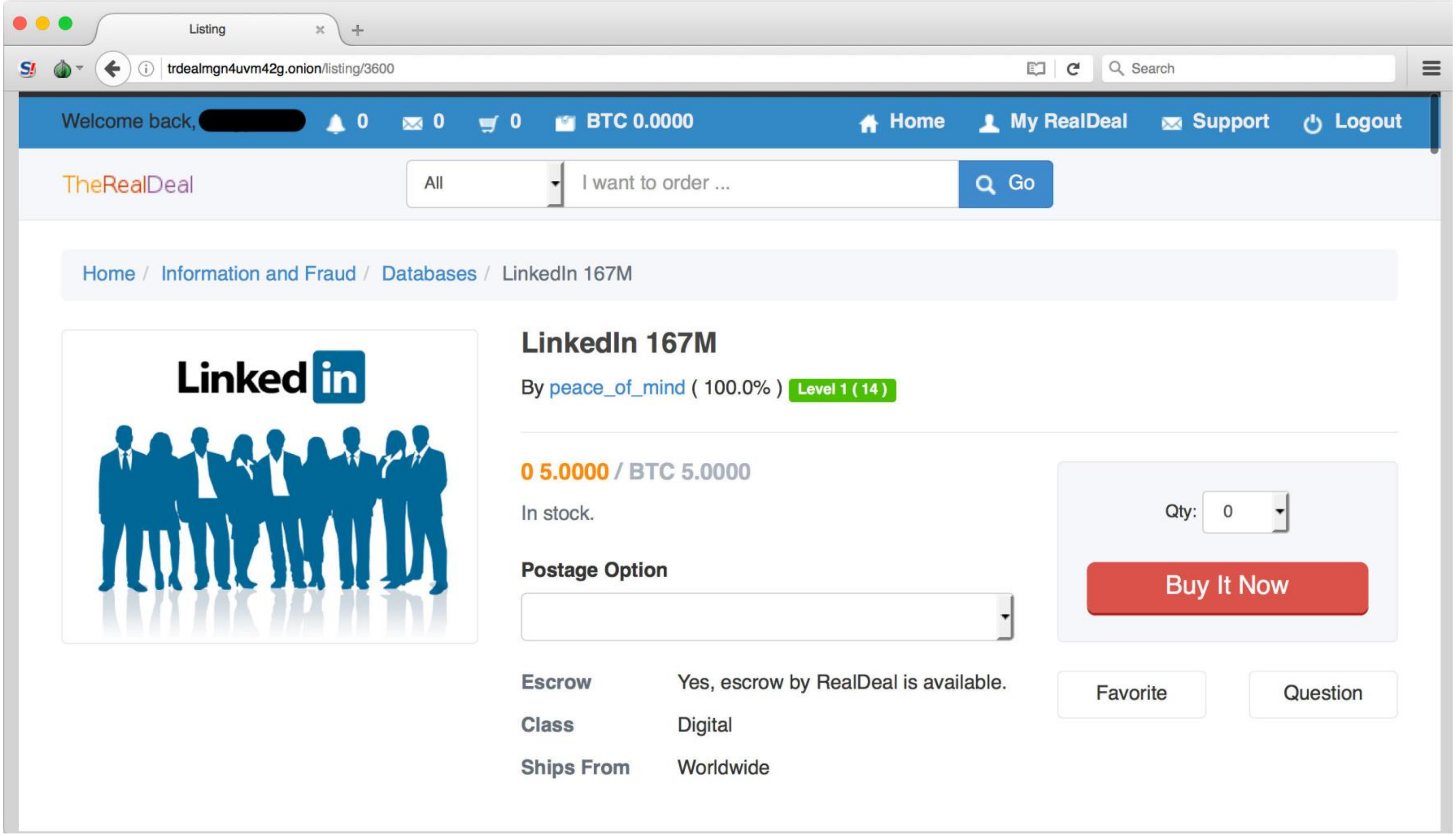
Email	Cracked
...	...
jim@mail.com	R0cky!17
...	...

1 guess is enough!

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
...	...

Monitoring the Black Market



Welcome back, [redacted] 0 0 0 BTC 0.0000 Home My RealDeal Support Logout

TheRealDeal All I want to order ... Go

Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

0 5.0000 / BTC 5.0000

In stock.

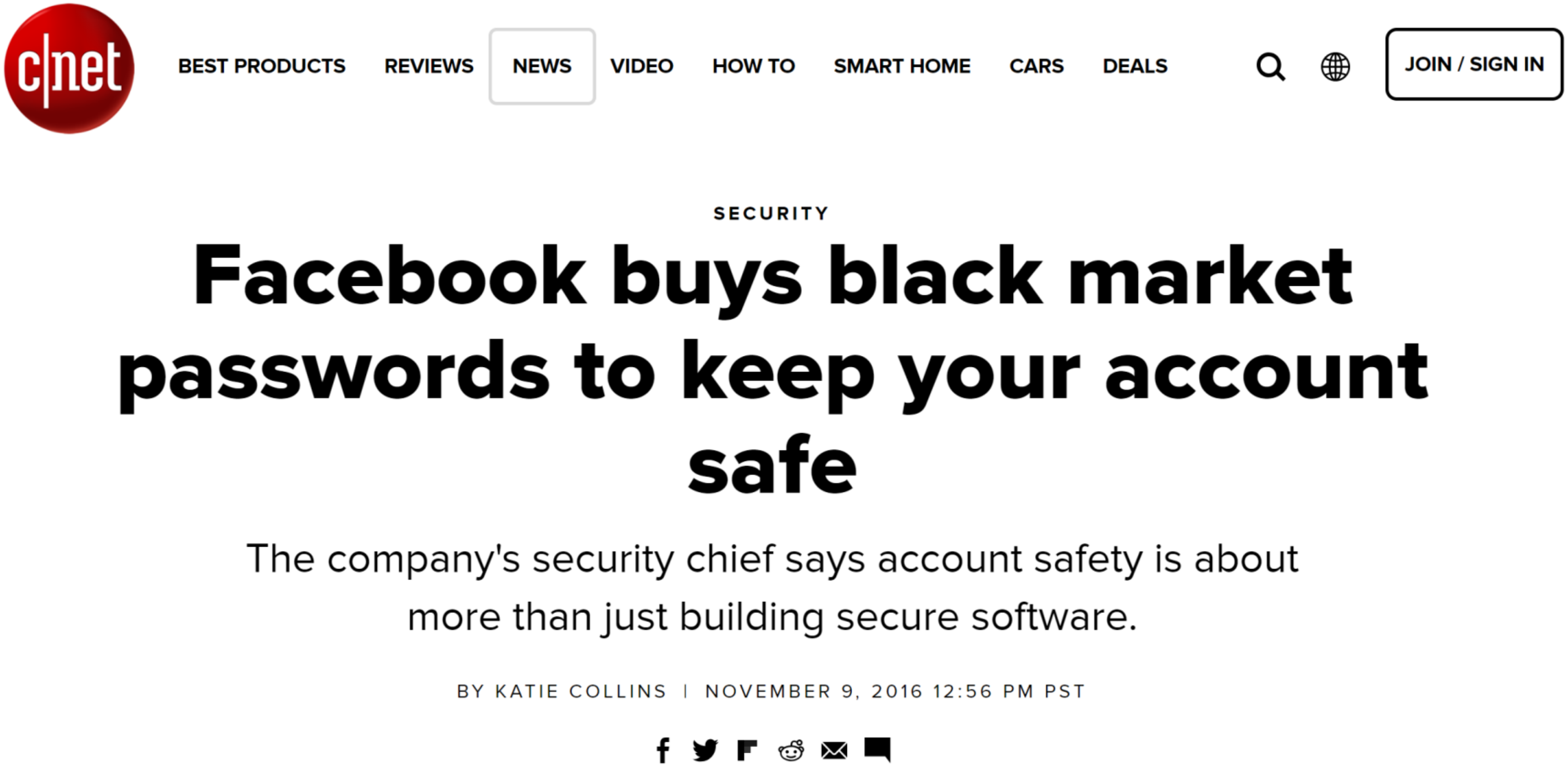
Qty: 0

Buy It Now

Postage Option

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

Favorite Question



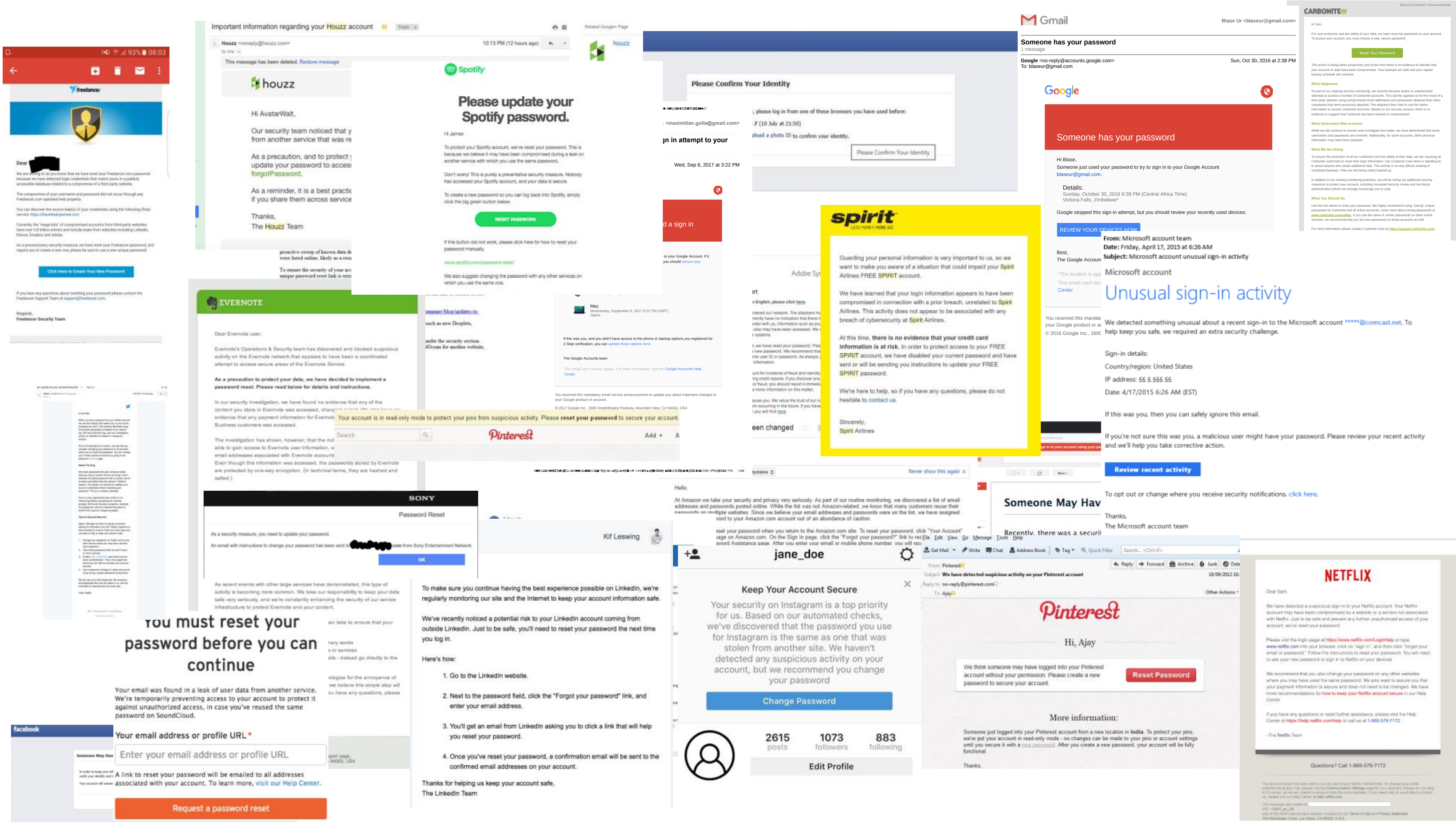
SECURITY

Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST

Password-Reuse Notifications



Important information regarding your Houzz account

Houzz <noreply@houzz.com> 10:13 PM (12 hours ago)

This message has been deleted. Restore message

houzz

Hi AvatarWalt,

Our security team noticed that y from another service that was re

As a precaution, and to protect y update your password to acces forgotPassword.

As a reminder, it is a best practic if you share them across service

Thanks,
The Houzz Team

Spotify

Please update your Spotify password.

Hi James

To protect your Spotify account, we've reset your password. This is because we believe it may have been compromised during a leak on another service with which you use the same password.

Don't worry! This is purely a preventative security measure. Nobody has accessed your Spotify account, and your data is secure.

To create a new password so you can log back into Spotify, simply click the big green button below.

RESET PASSWORD

If this button did not work, please click here for how to reset your password manually.

www.spotify.com/password-reset/

We also suggest changing the password with any other services on which you use the same one.

Please Confirm Your Identity

please log in from one of these browsers you have used before:

7 (10 July at 21:50)

Upload a photo ID to confirm your identity.

Please Confirm Your Identity

Gmail

Blase Ur <blaseur@gmail.com>

Someone has your password

1 message

Google <no-reply@accounts.google.com> Sun, Oct 30, 2016 at 2:38 PM
To: blaseur@gmail.com

Google

Someone has your password

Hi Blase,

Someone just used your password to try to sign in to your Google Account blaseur@gmail.com.

Details:
Sunday, October 30, 2016 9:38 PM (Central Africa Time)
Victoria Falls, Zimbabwe*

Google stopped this sign-in attempt, but you should review your recently used devices:

REVIEW YOUR DEVICES NOW

Best,
The Google Account

CARBONITE

Reset Your Password

freelancer

Dear [redacted]

Click Here to Create Your New Password

Regards,
Freelancer Security Team

EVERNOTE

Dear Evernote user,

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses associated with Evernote accounts and encrypted passwords. Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and salted.)

Your account is in read-only mode to protect your pins from suspicious activity. Please **reset your password** to secure your account.

Pinterest

spirit

Guarding your personal information is very important to us, so we want to make you aware of a situation that could impact your Spirit Airlines FREE SPIRIT account.

We have learned that your login information appears to have been compromised in connection with a prior breach, unrelated to Spirit Airlines. This activity does not appear to be associated with any breach of cybersecurity at Spirit Airlines.

At this time, **there is no evidence that your credit card information is at risk.** In order to protect access to your FREE SPIRIT account, we have disabled your current password and have sent or will be sending you instructions to update your FREE SPIRIT password.

We're here to help, so if you have any questions, please do not hesitate to contact us.

Sincerely,
Spirit Airlines

From: Microsoft account team
Date: Friday, April 17, 2015 at 6:26 AM
Subject: Microsoft account unusual sign-in activity

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account *****@comcast.net. To help keep you safe, we required an extra security challenge.

Sign-in details:
Country/region: United States
IP address: 55.5.555.55
Date: 4/17/2015 6:26 AM (EST)

If this was you, then you can safely ignore this email.

If you're not sure this was you, a malicious user might have your password. Please review your recent activity and we'll help you take corrective action.

Review recent activity

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

SONY

Password Reset

As a security measure, you need to update your password.

An email with instructions to change your password has been sent to [redacted] .com from Sony Entertainment Network.

OK

Kif Leswing

To make sure you continue having the best experience possible on LinkedIn, we're regularly monitoring our site and the Internet to keep your account information safe.

We've recently noticed a potential risk to your LinkedIn account coming from outside LinkedIn. Just to be safe, you'll need to reset your password the next time you log in.

Here's how:

1. Go to the LinkedIn website.
2. Next to the password field, click the "Forgot your password" link, and enter your email address.
3. You'll get an email from LinkedIn asking you to click a link that will help you reset your password.
4. Once you've reset your password, a confirmation email will be sent to the confirmed email addresses on your account.

Thanks for helping us keep your account safe,
The LinkedIn Team

You must reset your password before you can continue

Your email was found in a leak of user data from another service. We're temporarily preventing access to your account to protect it against unauthorized access, in case you've reused the same password on SoundCloud.

Your email address or profile URL *

Enter your email address or profile URL

A link to reset your password will be emailed to all addresses associated with your account. To learn more, visit our Help Center.

Request a password reset

Hello,

At Amazon we take your security and privacy very seriously. As part of our routine monitoring, we discovered a list of email addresses and passwords posted online. While the list was not Amazon-related, we know that many customers reuse their passwords on multiple websites. Since we believe your email addresses and passwords were on the list, we have assigned a temporary password to your Amazon.com account out of an abundance of caution.

jane_doe

Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password

Change Password

2615 posts 1073 followers 883 following

Edit Profile

Someone May Hav

Recently, there was a securit

From: Pinterest
Subject: We have detected suspicious activity on your Pinterest account
Reply to: no-reply@pinterest.com
To: Ajay

Pinterest

Hi, Ajay

We think someone may have logged into your Pinterest account without your permission. Please create a new password to secure your account.

Reset Password

More information:

Someone just logged into your Pinterest account from a new location in India. To protect your pins, we've put your account in read-only mode - no changes can be made to your pins or account settings until you secure it with a new password. After you create a new password, your account will be fully functional.

Thanks,

NETFLIX

Dear Sam,

We have detected a suspicious sign-in to your Netflix account. Your Netflix account may have been compromised by a website or a service not associated with Netflix. Just to be safe and prevent any further unauthorized access of your account, we've reset your password.

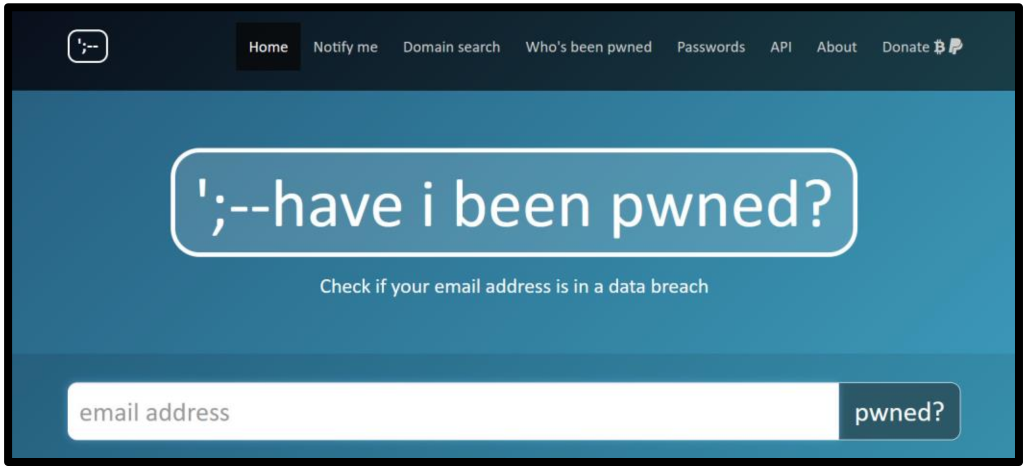
—The Netflix Team

Questions? Call 1-866-579-7172

facebook

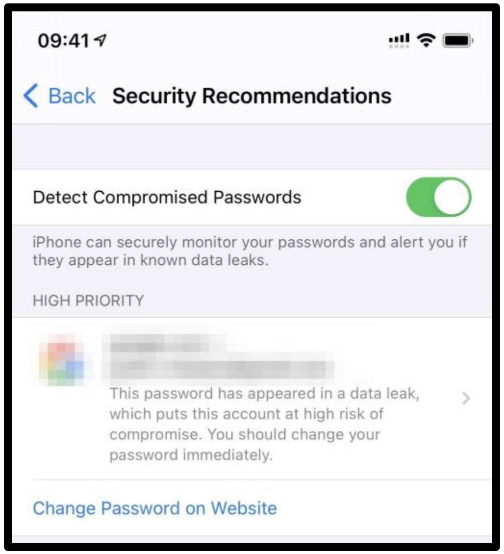
Authentication in Practice: Checking for Compromised Credentials

Checking for Compromised Credentials



';--have i been pwned?

Check if your email address is in a data breach



Security Recommendations

Detect Compromised Passwords

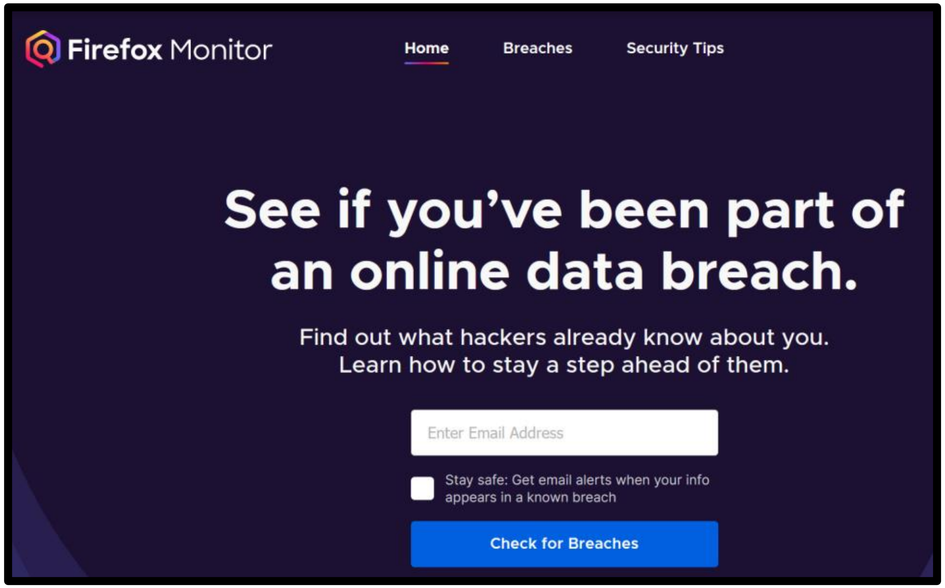
iPhone can securely monitor your passwords and alert you if they appear in known data leaks.

HIGH PRIORITY

[redacted]

This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.

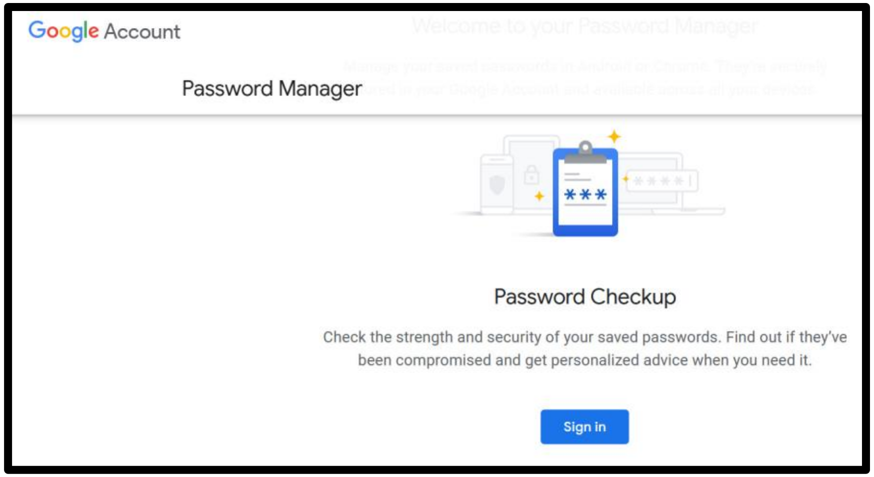
Change Password on Website



See if you've been part of an online data breach.

Find out what hackers already know about you.
Learn how to stay a step ahead of them.

□ Stay safe: Get email alerts when your info appears in a known breach



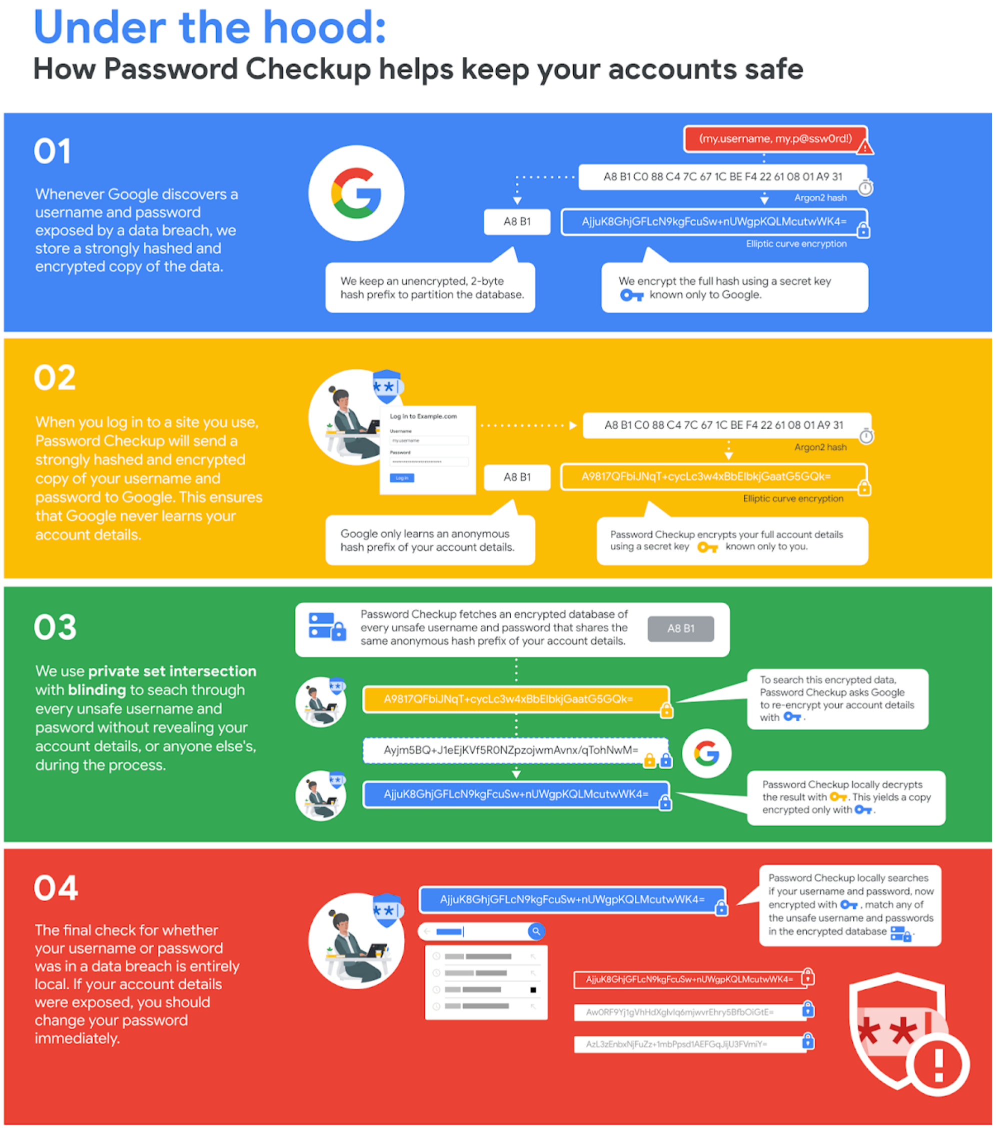
Password Manager

Password Checkup

Check the strength and security of your saved passwords. Find out if they've been compromised and get personalized advice when you need it.

https://www.zdnet.com/article/google-launches-password-checkup-feature-will-add-it-to-chrome-later-this-year/
https://ios.gadgethacks.com/how-to/ios-14-monitors-your-passwords-protect-you-against-data-breaches-heres-works-0341281/

Checking for Compromised Credentials



Under the hood:

How Password Checkup helps keep your accounts safe

01

Whenever Google discovers a username and password exposed by a data breach, we store a strongly hashed and encrypted copy of the data.

(my.username, my.p@ssw0rd!)
A8 B1 C0 88 C4 7C 67 1C BE F4 22 61 08 01 A9 31
Argon2 hash
A8 B1
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
Elliptic curve encryption

We keep an unencrypted, 2-byte hash prefix to partition the database.

We encrypt the full hash using a secret key 🔑 known only to Google.

02

When you log in to a site you use, Password Checkup will send a strongly hashed and encrypted copy of your username and password to Google. This ensures that Google never learns your account details.

Log in to Example.com
Username
my.username
Password
Log in
A8 B1 C0 88 C4 7C 67 1C BE F4 22 61 08 01 A9 31
Argon2 hash
A8 B1
A9817QFbiJNqT+cycLc3w4xBbElbkjGaatG5GQk=
Elliptic curve encryption

Google only learns an anonymous hash prefix of your account details.

Password Checkup encrypts your full account details using a secret key 🔑 known only to you.

03

We use **private set intersection** with **blinding** to seach through every unsafe username and pasword without revealing your account details, or anyone else's, during the process.

Password Checkup fetches an encrypted database of every unsafe username and password that shares the same anonymous hash prefix of your account details.

A8 B1
A9817QFbiJNqT+cycLc3w4xBbElbkjGaatG5GQk=
Ayjm5BQ+J1eEjKVf5R0NZpzojwmAvnx/qTohNwM=
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=

To search this encrypted data, Password Checkup asks Google to re-encrypt your account details with 🔑.

Password Checkup locally decrypts the result with 🔑. This yields a copy encrypted only with 🔑.

04

The final check for whether your username or password was in a data breach is entirely local. If your account details were exposed, you should change your password immediately.

AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
Aw0RF9Yj1gVhHdXglvlq6mjwvrEhry5BfbOiGtE=
AzL3zEnbxNjFuZz+1mbPpsd1AEFGqJijU3FVmiY=

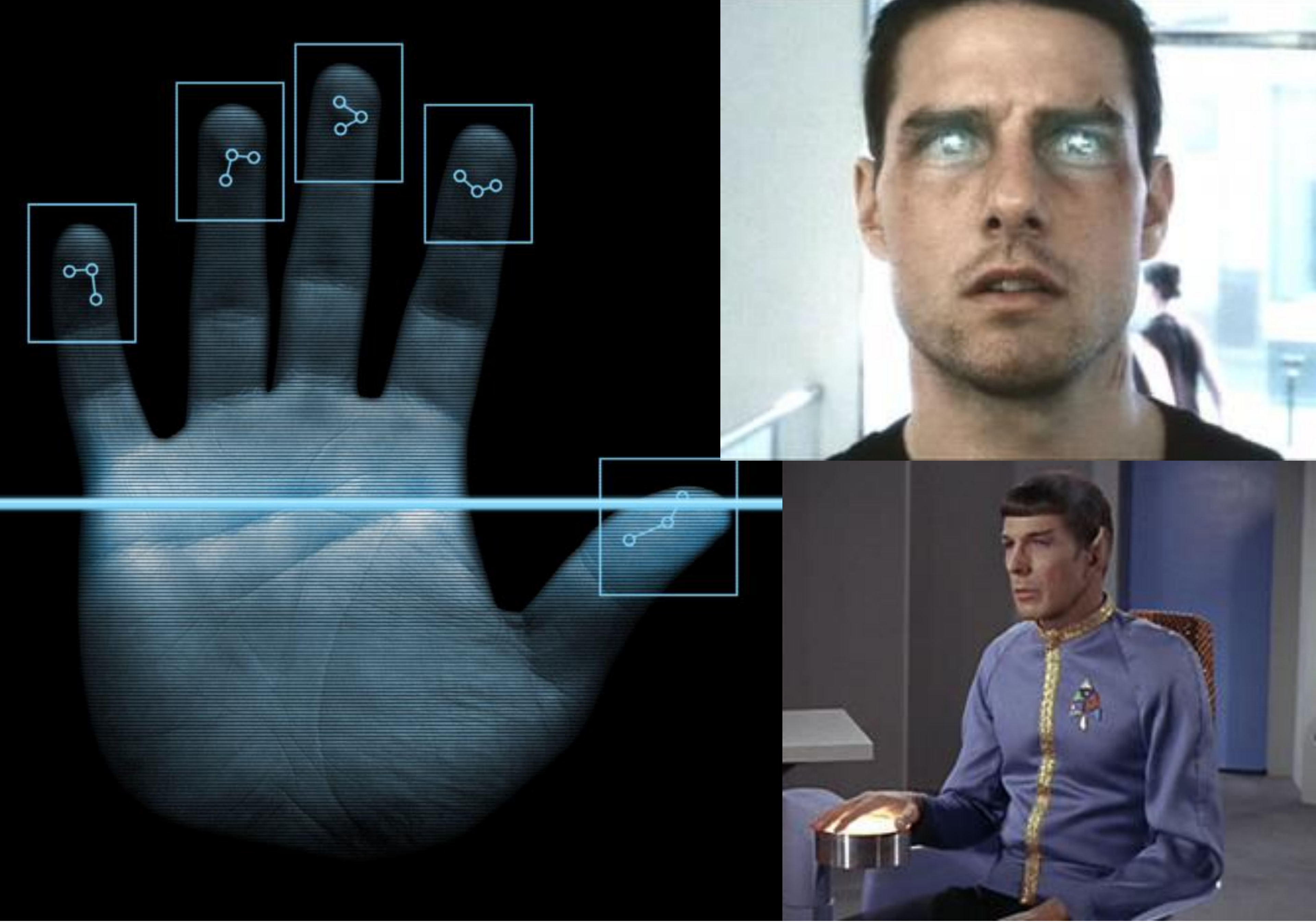
Password Checkup locally searches if your username and password, now encrypted with 🔑, match any of the unsafe username and passwords in the encrypted database 🗄.

https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html

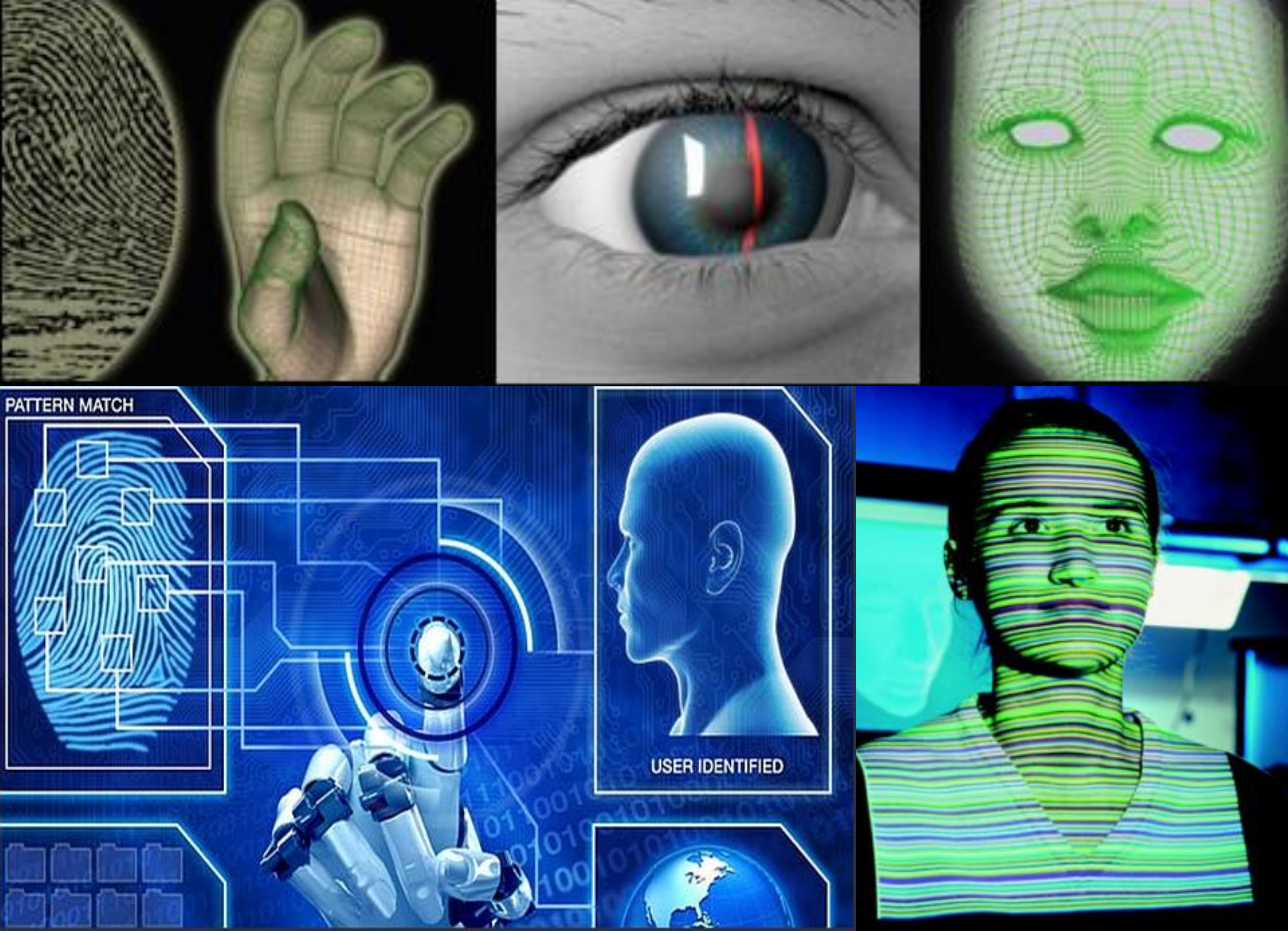
What about Biometrics?

nages on previous slide fair use from androidcentral.com and businessinsider.com. Photo above fair use from abcnews.com

nages fair use from wordpress.com and kaspersky.com, as well as Creative Commons from matsuyuki on Flickr



mages fair use from ccmcinc.com, filmjunk.com, and discovermagazine.com



Images fair use from fbi.gov, ifsecglobal.com, and siemens.com

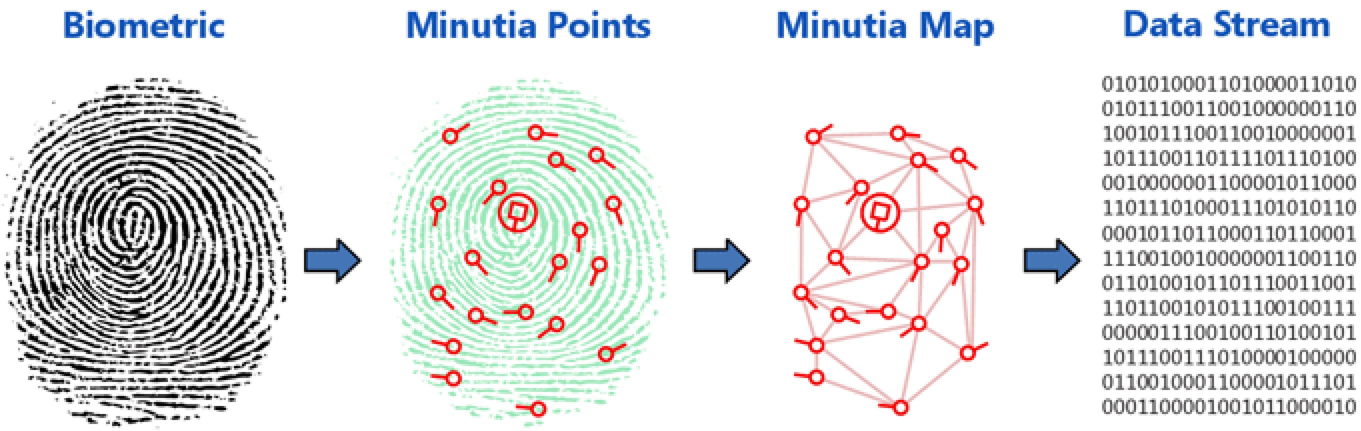
Biometrics

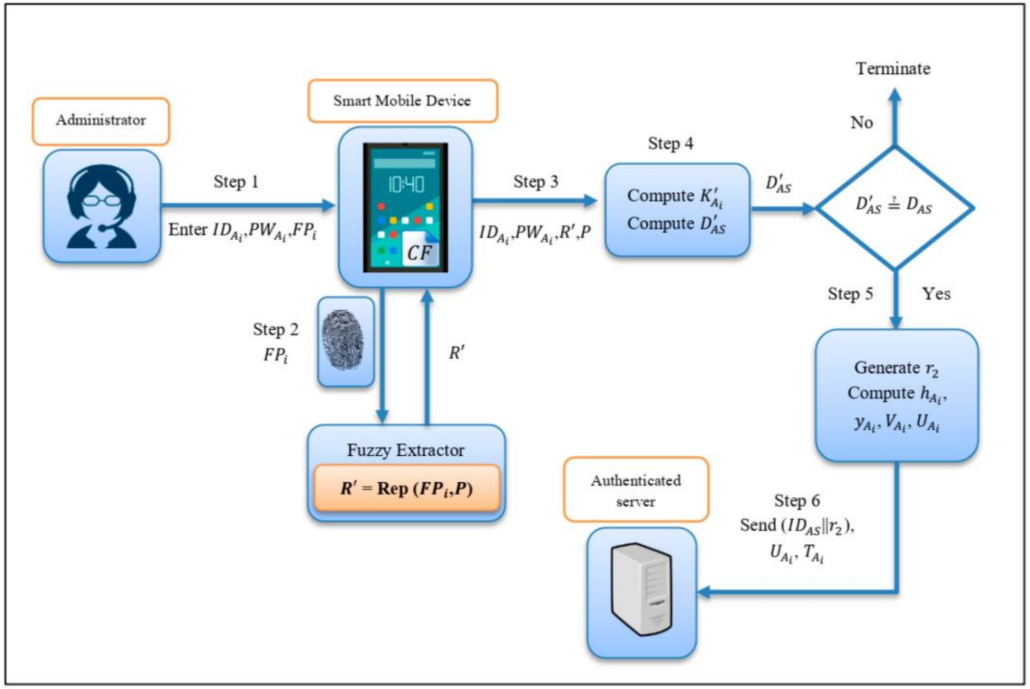
- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

Practical Challenges for Biometrics

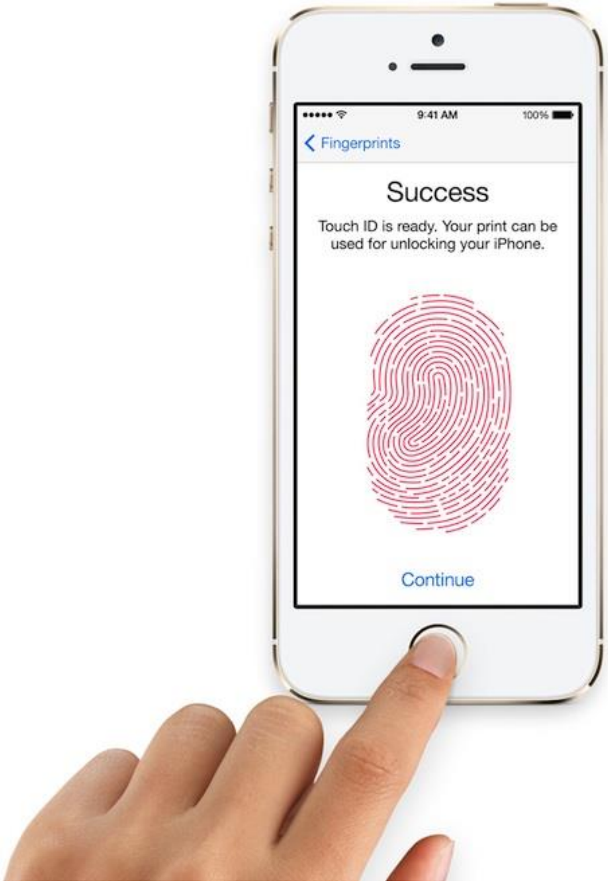
- Immutable (can’t be changed)
- Potentially sensitive data
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time

Storing Biometrics: Templates





iPhone Touch ID



Success

Touch ID is ready. Your print can be used for unlocking your iPhone.

Android Face Unlock

•Images fair use from androidcentral.com, creativebits.org, and businessinsider.com.

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter their password
- Falls back to the password
- Face recognition can be tricked by a photo
- Fingerprint recognition can be tricked by a gummy mold
- Users find fingerprint unlock convenient, but do not particularly like face unlock

Authentication Conclusions

- Authentication is really hard!
  - Hard for system administrators
  - Hard for users
- Unfortunately, authentication is necessary

Access Control

Access Control: Basic Instantiation

- File permissions on UNIX:
  - Owner, Group, Others
- Useful commands
  - chown (**ch**ange **own**er of a file)
    - chown blase:plantnerds rareplants.txt
  - chmod (**ch**ange **mod**es of a file)
    - chmod g+w rareplants.txt (**u**ser **g**roup **o**thers, add **+** or remove **-**, **r**ead **w**rite e**x**ecute)
    - chmod 750 rareplants.txt (additive: 0 = nothing, 1 = execute, 2 = write, 4 = read)

Access Control

- Role-based access control
  - Authorization based on role (e.g., “UChicago student”)
- Attribute-based access control
  - Authorization based on attribute(s) (e.g., “Over 7 feet tall”)
- Context-based access control
  - Authorization decision depends on the context (e.g., time of day)