
Passwords and Human Authentication

15 May 2025
Lecture 7

Some Slides Credit: Steve Zdancewic (UPenn)

Topics for Today

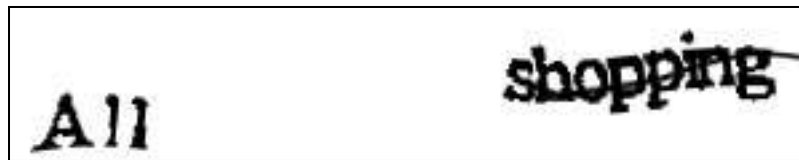
- Human Authentication
 - Password basics
 - Multi-factor authentication
 - Password storage
 - Password alternatives

Human User Authentication

- How do you:
 - Know you're talking to a human?
 - Allow a human user to identify him or herself to a machine?
- Machine
 - Good at authenticating other machines
 - Good at mathematical manipulations, etc.
 - Can handle keys, secrets, etc.
 - Very good memory of things stored in it
- Humans
 - Good at identifying people
 - Use small clues that when combined yield an unmistakable picture
 - Voice
 - Height
 - Stance
 - Shared history

Identifying Any Human

- Problem:
 - How does a machine establish that it's talking to a human?
 - Why?
 - Prevent SPAM, abuse of web accounts, foil bots and web crawlers,...
- Answer: Challenge / Response
 - Challenge is something that only humans can do (quickly):
 - Example: deciphering obscured text



- Read: "Telling Humans and Computers Apart" (von Ahn, Blum, and Langford) www.captcha.net
- Counter strategies:
 - 'Grandmaster chess attack' : get humans to do the decoding

ReCaptcha



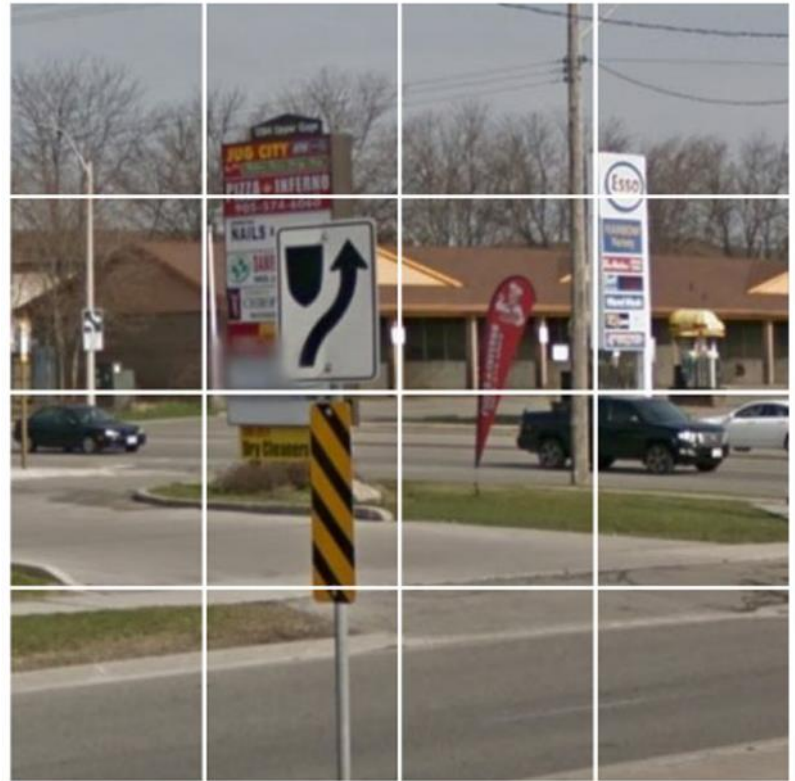
I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)

Select all squares with **street signs**.
If there are none, click skip.



SKIP

Identifying a particular human

Something you
know

Password, etc.



Something you
have

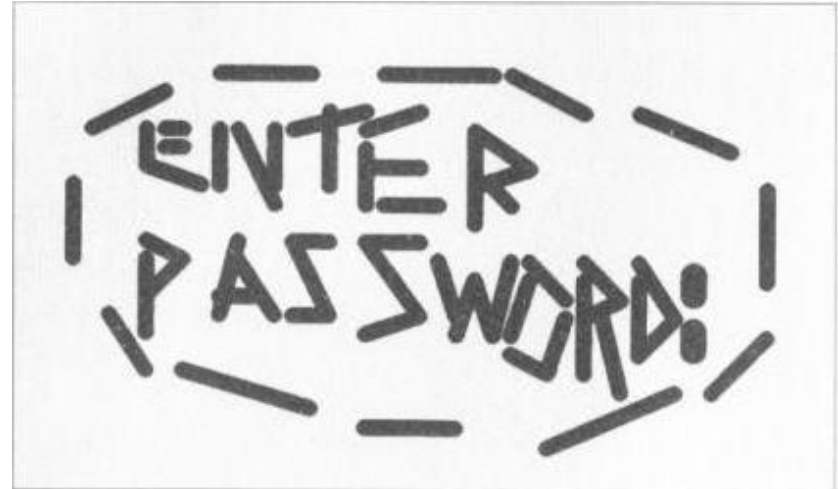
Driver's license, Student
ID, Key



Something
inherent about you
Biometric, location



Passwords

- Shared code/phrase
- Client sends to authenticate
- Simple, right?
- How do you...
 - 🏢 Establish them to begin with?
 - ☁️⬇️ Stop them from leaking?
 - Stop them from being guessed?



SOURCE: NASA

Prime Mover Problem

- Set up password: out of band
 - Physical mail 
 - Email 
 - Attached to the box
 - SMS
- Piggybacking
 - Swipe ID Card to make Password
 - But where does the chain stop?
 - ID Card → TZ → birth certificate



On the box

Model name: Bright Box Wireless Router

Wireless network name:
EE-Bright-Box-xyhy

Wireless password:
gum-sleep-free

Router login details: <http://192.168.1.1>
Username: admin
Password: q7pfeg

MAC XXXXXXXXXXXXX



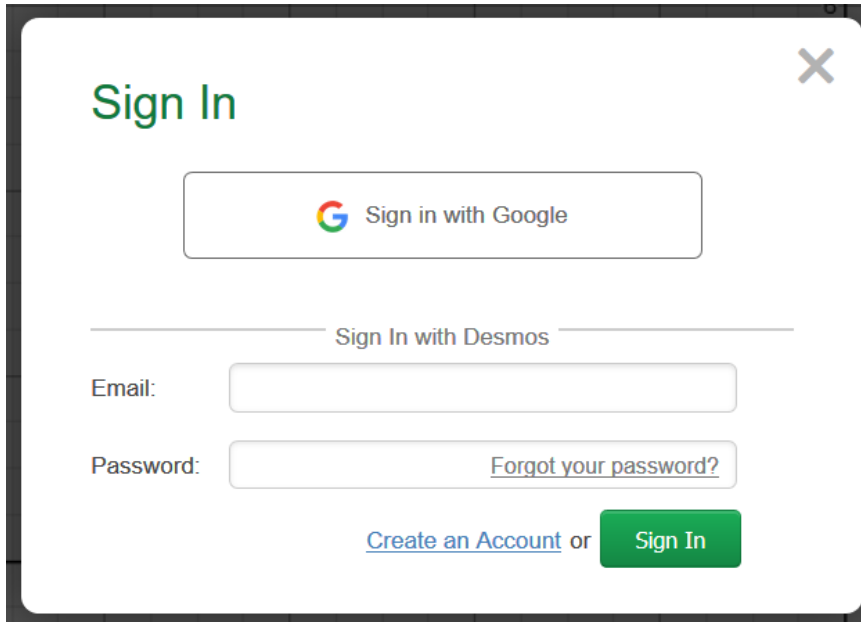
Serial No. XXXXXXXXXXXXX



ASTORIA
networks

Made in XXX 146000107400J R01 XX

Federated ID (Oauth)



A modal window titled "Sign In" with a close button (X) in the top right corner. It features a "Sign in with Google" button at the top. Below it, a horizontal line separates the Google login from the "Sign In with Desmos" section. This section includes an "Email:" label and a text input field, a "Password:" label and a text input field with a "Forgot your password?" link inside, and a "Create an Account" link followed by an "or" and a green "Sign In" button.

Sign In

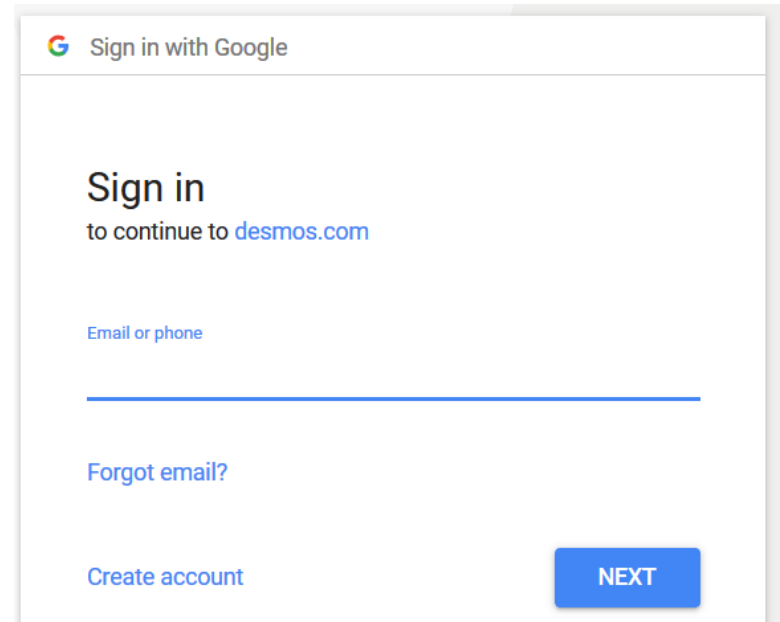
Sign in with Google

Sign In with Desmos

Email:

Password: [Forgot your password?](#)

[Create an Account](#) or [Sign In](#)



A web page titled "Sign in with Google" at the top. The main heading is "Sign in" followed by "to continue to [desmos.com](#)". Below this is a label "Email or phone" and a text input field. Further down are links for "Forgot email?" and "Create account". A blue "NEXT" button is located at the bottom right.

Sign in with Google

Sign in
to continue to [desmos.com](#)

Email or phone

[Forgot email?](#)

[Create account](#)

NEXT

How OAuth 2.0 Works

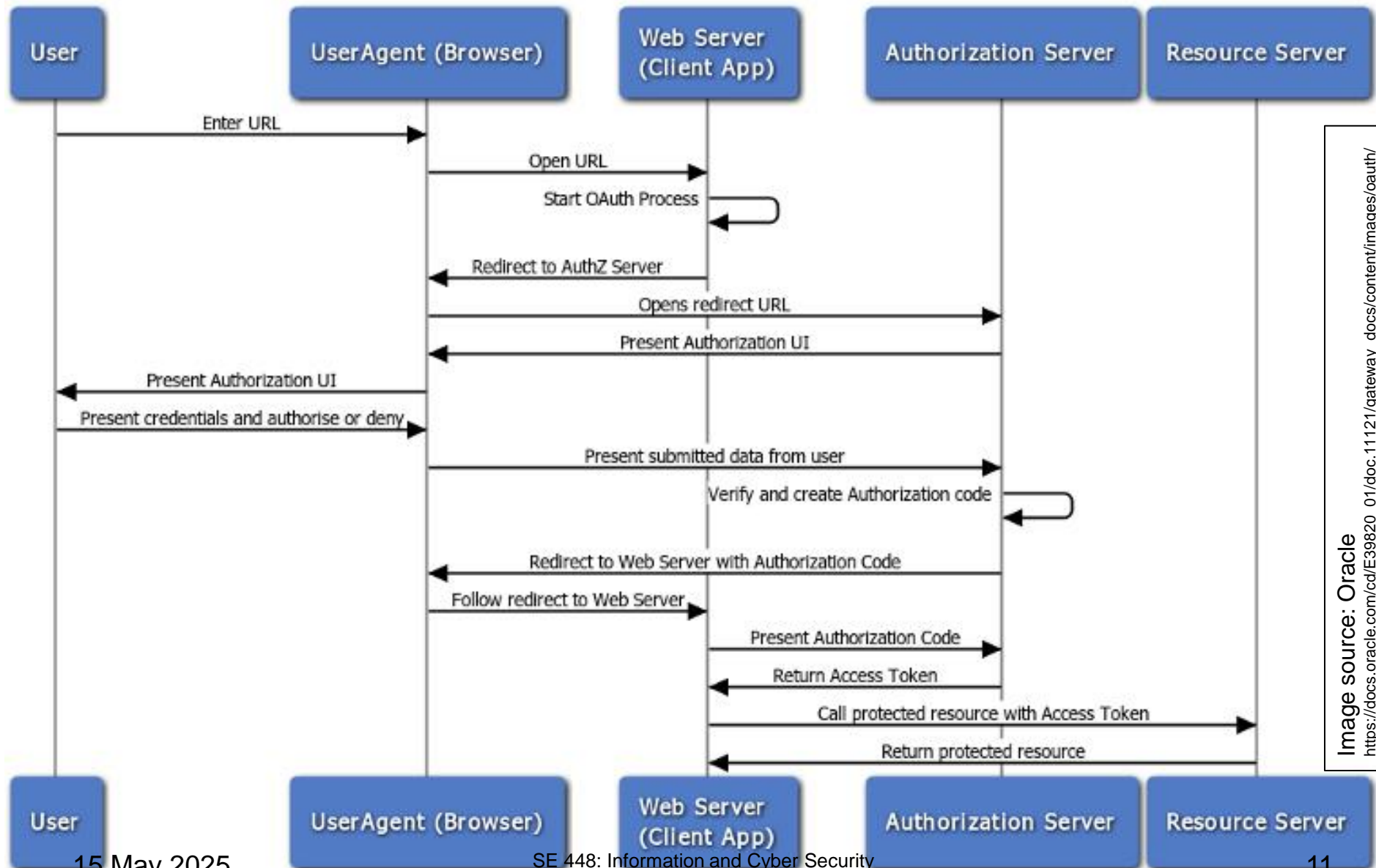


Image source: Oracle
https://docs.oracle.com/cd/E39820_01/doc.11121/gateway_docs/content/images/oauth/oauth_web_server_flow.png

Leaks & Challenges

- Social engineering
- Managing large numbers of passwords:
 - Writing the password down on paper
 - Storing it in an electronic "safe"
 - Using a web browsers 'remember this password' feature
- Legal and responsibility
 - Shared password == shared liability

Oops



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE F

TRANSLATES TO "THE PASSWORD OF DUM-DUM" —

Hacked French network exposed its own passwords during TV interview

Post-it note on wall revealed network's passwords for YouTube, Instagram.

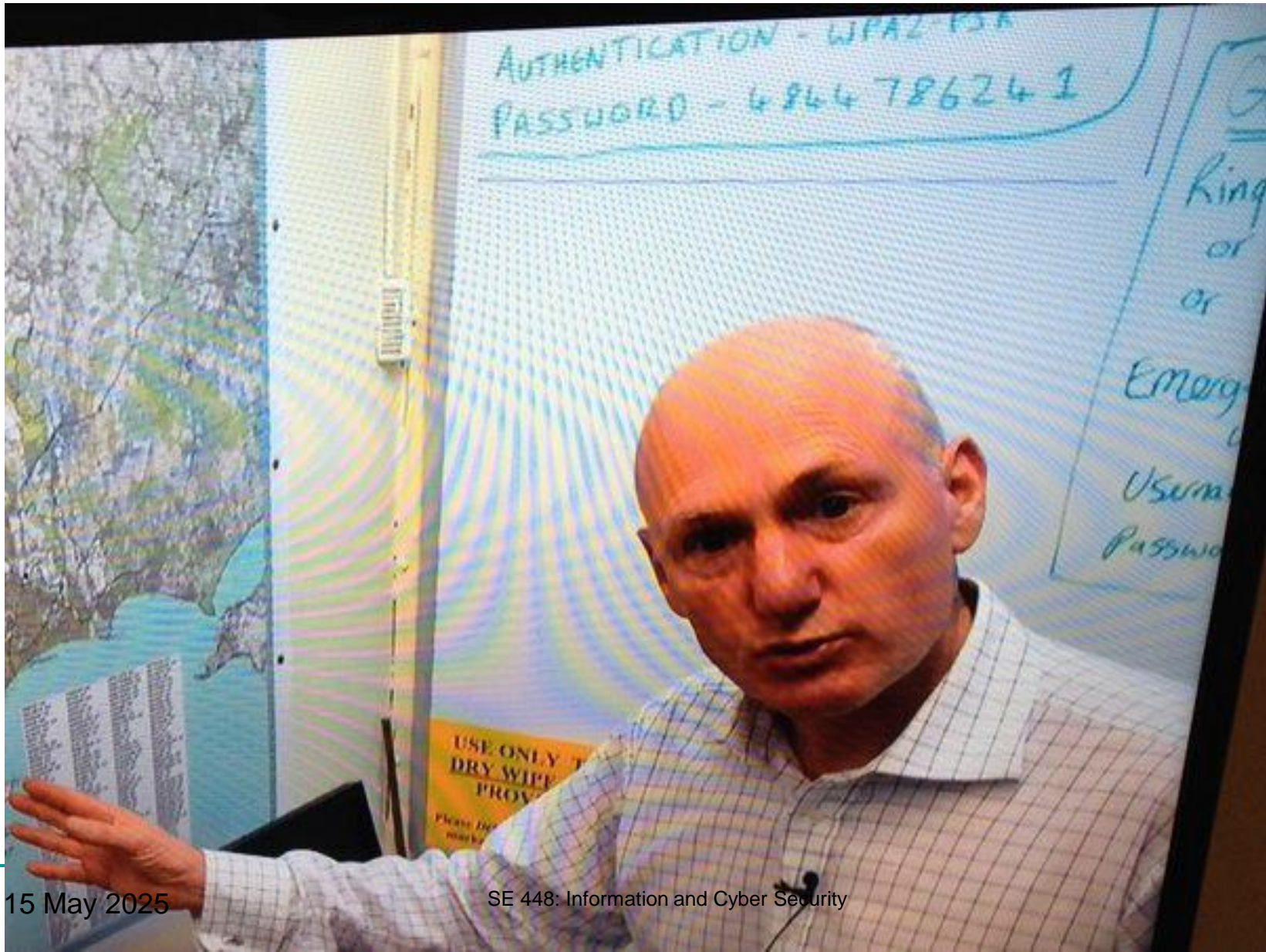
SAM MACHKOVECH - 4/10/2015, 4:37 AM



Oops



Oops



Oops



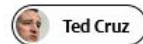
Oops

BUSINESS
INSIDER

WATCH: Sen. Ted Cruz tells Democratic Sen. Richard Blumenthal to change his iPhone passcode after he enters it in on live TV

Sonam Sheth

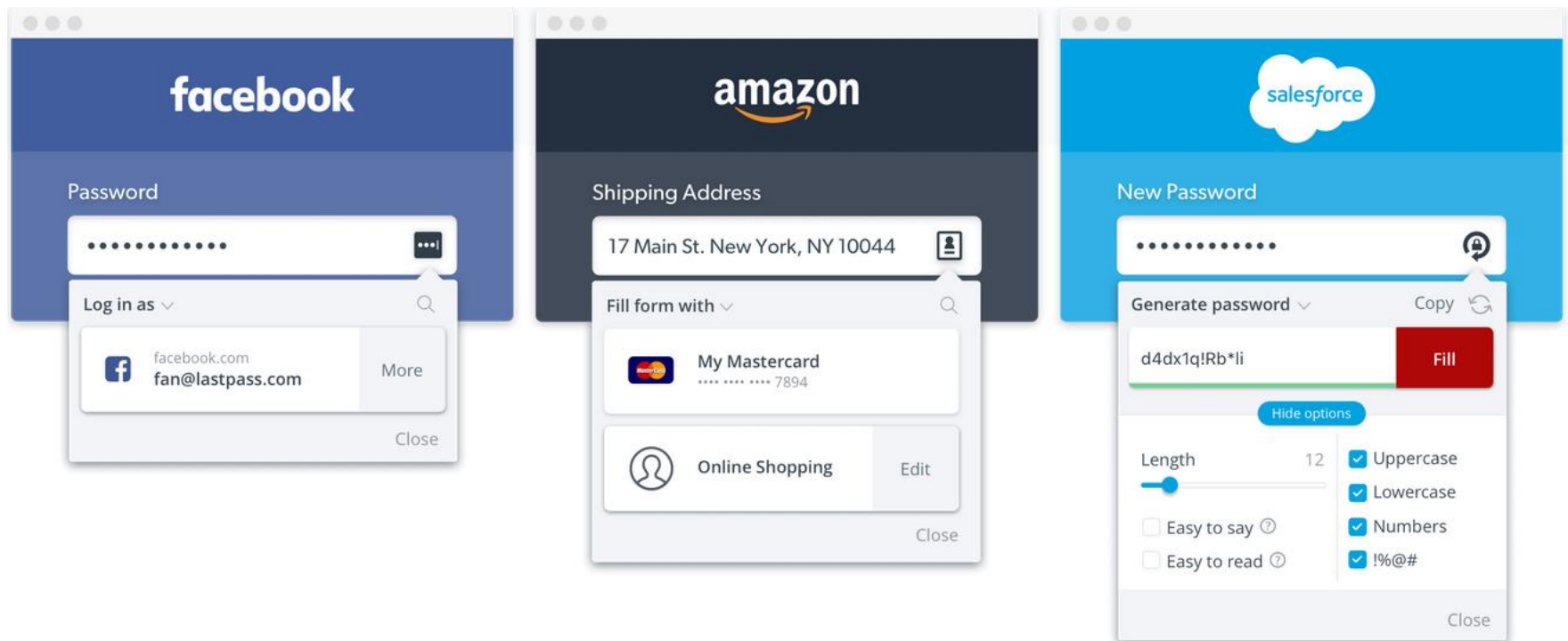
Wed, May 26, 2021, 12:05 AM · 2 min read



Sen. Richard Blumenthal holds up his iPhone during a subcommittee hearing on gun violence.

Screenshot/C-SPAN

Password Safe (LastPass)



Unless this happens

Home / Software / How-To

LastPass was hacked: Here's what you have to do

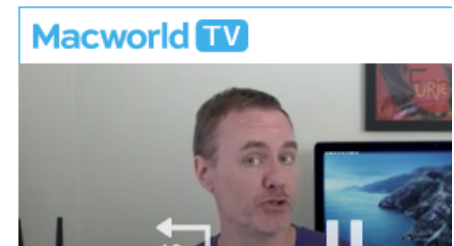
LastPass had the worst thing happen, but don't panic: You're still in the clear and your password is likely not cracked.



PRIVATE I

By [Glenn Fleishman](#), Senior Contributor | JUN 16, 2015 9:19 PM PDT

The password-storage maker [LastPass announced](#) the worst possible news for a company in its business on Monday: [its password database was breached](#) and user account information stolen. Because LastPass allows central storage and synchronization of your data store—the “vault” of passwords and other information you use with its app and website—someone being able to suss out your master password would seemingly have access to all your secrets.



Unless this happens (again)

Sep 16, 2019, 04:25am EDT | 249,736 views

Google Warns LastPass Users Were Exposed To 'Last Password' Credential Leak



Davey Winder Senior Contributor @

[Cybersecurity](#)

I report and analyse breaking cybersecurity and privacy stories



Google Project Zero has found a credential leaking vulnerability in the LastPass password manager. GETTY IMAGES

But don't worry, it's not that bad really

Unless this happens (again!!)

INDUSTRY NEWS • ⌚ 2 min read • 📌

LastPass Master Passwords Compromised in Mystery Attack



Filip TRUȚĂ
December 29, 2021

Ad One product to protect all your devices, without slowing them down.
[Free 90-day trial](#)

<https://www.bitdefender.com/blog/hotforsecurity/lastpass-master-passwords-compromised-in-mystery-attack/>

Company claims it was a
mistake

Unless this happens (again!!!)



CYBERSECURITY **DIVE**

[Deep Dive](#) [Library](#) [Press Releases](#)

[Strategy](#) [Breaches](#) [Vulnerability](#) [Cyberattacks](#) [Threats](#) [Leadership & Careers](#) [Partners](#)

What we know about the LastPass breach (so far)

The blast radius from a breach at LastPass grew from bad to worse during a four-month period. Most of the data held by the password manager is now compromised.

Published Jan. 5, 2023



[Matt Kapko](#)
Reporter



Summaries



Deep Dive Library Press Releases

Strategy Breaches Vulnerability Cyberattacks Threats Leadership & Career

LastPass breach timeline: How a monthslong cyberattack unraveled

A threat actor evaded detection for months and blended in with legitimate activity after targeting 1 of 4 engineers with access to keys to the kingdom.

Published March 2, 2023 • Updated March 3, 2023



Matt Kapko
Reporter



WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN

SECURITY DEC 28, 2022 2:53 PM

Yes, It's Time to Ditch LastPass

The password manager's most recent data breach is so concerning, users need to take immediate steps to protect themselves.

It's not over even 3 years later



CISO STORIES

TOPICS

TOPIC HUBS

EVENTS

PODCASTS

RESEARCH

REC

Identity, Threat Intelligence, Application security

LastPass hack leveraged to facilitate \$150M crypto heist

March 10, 2025

 Share

By [SC Staff](#)



Guessing Passwords

User Problems

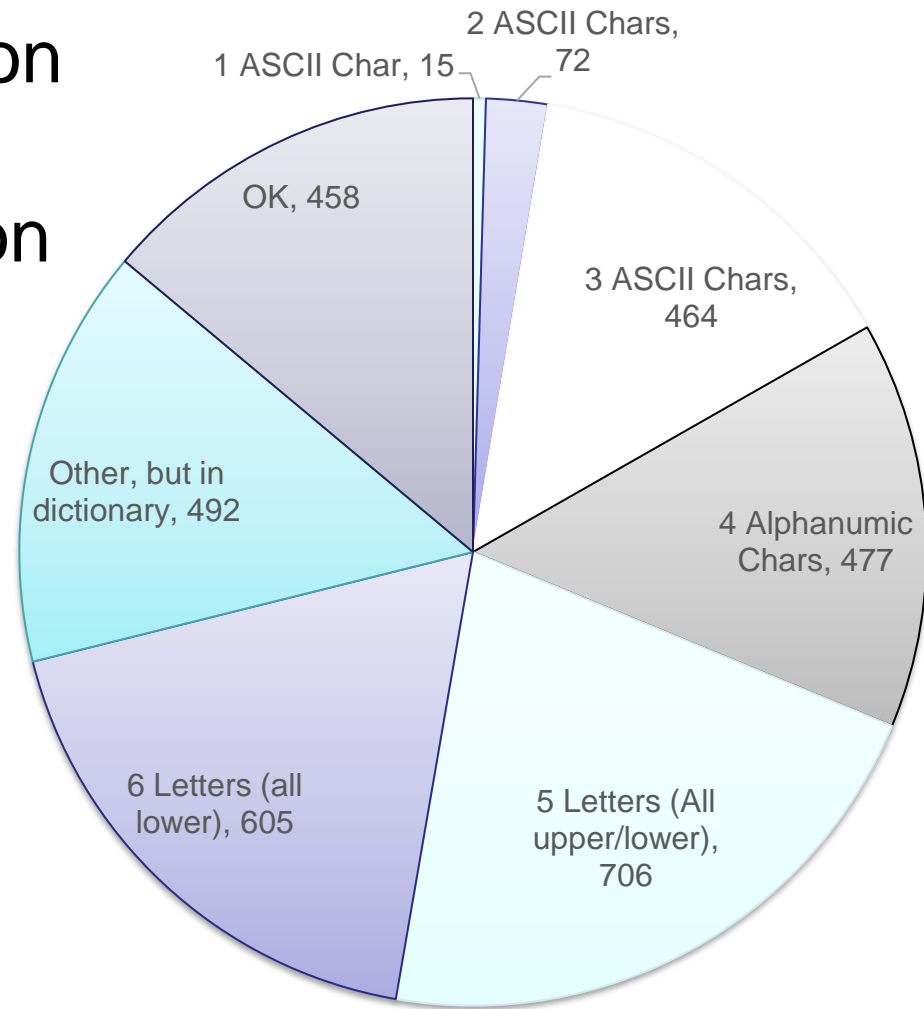
- “No such user” error
 - Gives an attacker information about usernames
 - “User or password are incorrect”
- “Here's who we are” mistake
 - Gives an attacker information about usernames

Password Problems

- Common words, phrases for passwords
- Null passwords, "password", username, backwards, etc.
- Dictionary attacks
- How bad is it?

1979 Survey of 3,289 Passwords

- With no constraints on choice of password, Morris and Thompson got:



Other Surveys of Passwords

Klein (1990) and Spafford (1992) of 15K passwords

- 2.7% guessed in 15 minutes, 21% in a week
- Sounds ok? Not if the passwords last 30 days

Adobe (2013) “survey” of 153,000,000 passwords:

- Top 100 passwords
(<http://www.whatsmypass.com/top-100-adobe-passwords>)
- Top 10: *123456, 123456789, password, adobe123, 12345678, qwerty, 1234567, 111111, photoshop, 123123*

Schneier (2006) survey of 34,000 MySpace passwords

- 65% eight characters or less
- 28% lower case letters followed by a single digit
- Top 11 passwords: *password1, abc123, myspace1, password, blink182, qwerty1, f***you, 123abc, baseball1, football1, 123456*
- 23% could be cracked in 30 min, 55% in 8 hours

Other Surveys of Passwords

- NordPass (2020) survey of Israeli cracked passwords

1	123456	167,776
2	123456789	53,971
3	1234	38,537
4	12345	35,581
5	123123	32,526
6	12345678	23,238
7	password	19,667
8	1234567	14,561
9	111111	13,298
10	1q2w3e4r	13,188

XKCD

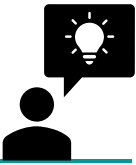
HACKERS RECENTLY LEAKED **153 MILLION** ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.

ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER	PASSWORD	HINT	
4e18acc1ab27a2d6		WEATHER VANE SWORD	<input type="text"/>
4e18acc1ab27a2d6			<input type="text"/>
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1	<input type="text"/>
8babbb6299e06eb6d		DUH	
8babbb6299e06eb6d	a0a2876eb1ea1fca		<input type="text"/>
8babbb6299e06eb6d	85e9da81a8a78adc	57	
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES	
1ab29ae86dabe5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS	
a1f9b2b6299e7a2b	codec1e6ab797397	SEXY EARLOBES	<input type="text"/>
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE	<input type="text"/>
39738b7adb0b8af7	617ab0277727ad85	SUGARLAND	
1ab29ae86dabe5ca		NAME + JERSEY #	
877ab7889d3862b1		ALPHA	<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1			<input type="text"/>
877ab7889d3862b1		OBVIOUS	<input type="text"/>
877ab7889d3862b1		MICHAEL JACKSON	<input type="text"/>
38a7c9279codeb44	9dca1d79d4dec6d5		
38a7c9279codeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE	<input type="text"/>
38a7c9279codeb44		PURLOINED	<input type="text"/>
a8ae5745a2b7af7a	9dca1d79d4dec6d5	FAV. LIAISON - 3 POKEMON	<input type="text"/>

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

Password Hacks



Tricks

- Letter substitutions, words backwards, common names, patterns, etc.
- Anything you can think of off the top of your head, a hacker can think of too

Lazy users!

- Weakest link is always the way of the attack
- One weak password is enough to give access

Heuristics for Guessing Attacks

Dictionary

- Words spelled backwards too
- Israel bonus: Hebrew words spelled in English
- Sample dictionary:
<https://www.scrapmaker.com/view/dictionaries/rockyou.txt>

Names (upper + lower)

- First names (best obtained from some mailing list). (Upper + lower)
- Last names
- Street names
- City names.

License plate numbers in your area. (About 5 hours work in 1979 for New Jersey.)

Room numbers, social security numbers, telephone numbers, etc.

Password crackers

John the
ripper

Hashcat

Medusa

THC Hydra

RainbowCrack

And many more. And these are just the public ones.

What makes a good password?



Password Length

- 64 bits of randomness is hard to crack
 - About 20 common ASCII characters
- But... People can't remember random strings
- Longer not necessarily better - people reuse or write passwords

Pass phrases

- English Text has roughly 1.3 random bits/char.
- Thus about 50 letters of English text
- Hard to type without making mistakes!

What makes a good password?



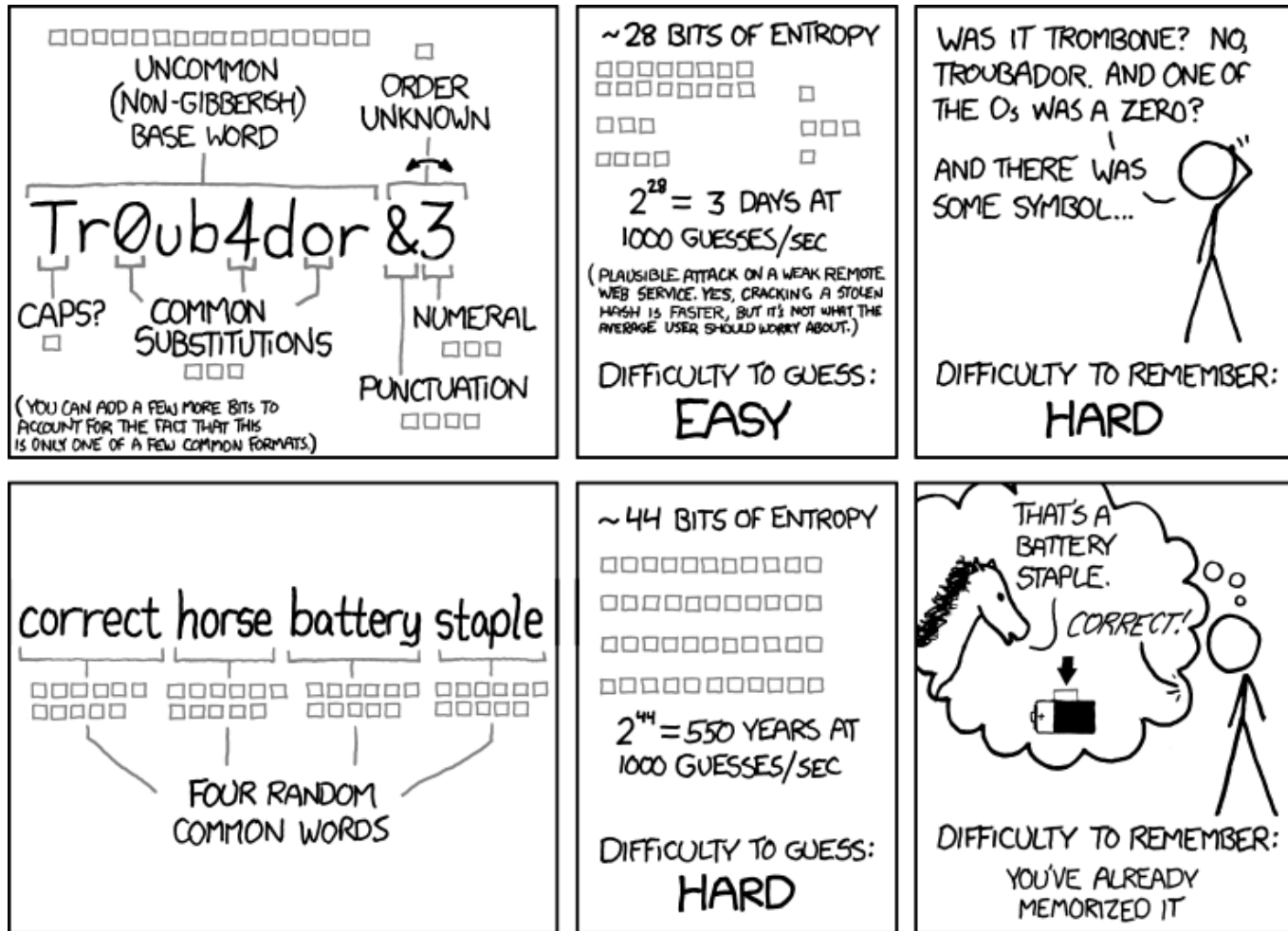
In practice

- Non-dictionary, mixed case, mixed alphanumeric
- Not too short (or too long)
8 - 12 characters
- Tools that check password strength
 - <https://howsecureismypassword.net/>
- Enforce non-reuse and expiration

Infographic

- <https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic>

Password Entropy



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

So Far

- Human Authentication
 - Password basics
 - Multi-factor authentication
 - Password storage
 - Password alternatives

Multifactor Authentication (MFA)

Principle: Encrypt the time



Principle: Encrypt a base secret



Principle: Smart card
online public key



Aside: SMS for MFA

כניסה לאזור אישי

כניסה עם

שם משתמש וסיסמה

הודעת SMS

תעודת זהות

טלפון נייד

המשך

☐ אני מאשר/ת את תנאי השימוש

דף הבית > מגדל שלי > כניסה למגדל שלי

כניסה למגדל שלי

הזן ת.ז. 9 ספרות כולל ספרת ביקורת

במידה ואינך רשום תועבר לתהליך הרשמה מהירה

ברצוני לקבל את קוד הכניסה ל: ☐ נייד ☐ מייל

לכניסה עם ת.ז. או דרכון + סיסמה

המשך

Image sources: <https://www.yl-invest.co.il/>, <https://www.migdal.co.il/mymigdal/process/login>

Not such a good idea



COVID-19 BEST PRODUCTS ▾ REVIEWS ▾ NEWS ▾ HOW TO ▾ FINANCE ▾ HEALTH ▾ SMART HOME ▾ CARS ▾ DEALS ▾ DOWNLOAD 5G

<https://www.cnet.com/how-to/do-you-use-sms-for-two-factor-authentication-heres-why-you-shouldnt/>

Do you use SMS for two-factor authentication? Here's why you shouldn't

Using two-factor authentication, or 2FA, is the right thing to do. But you put yourself at risk getting codes over text. We explain why.



Matt Elliott April 8, 2020 10:00 a.m. PT

<https://www.howtogeek.com/310418/why-you-shouldnt-use-sms-for-two-factor-authentication/>



Customers Solutions ▾ Products ▾ Services ▾ Resources ▾ Company ▾

Phone numbers as identifiers: The problem with SMS-based authentication



Marc Rogers
Executive Director of Cybersecurity

February 14, 2019

I recently heard about a Facebook user who encountered a very concerning login experience. After entering a password recovery code he had received via SMS, the user was accidentally logged into someone else's Facebook account.

The phone number the user had used to receive the SMS was actually a recycled number that previously belonged to someone else. Because the original owner of that number never disassociated it from his Facebook account, an SMS-based login attempt made with that number resulted in a login to that account. Not ideal, to say the least.

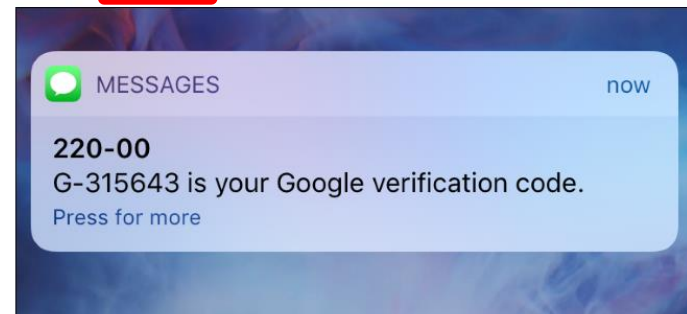


NEWS FEATURES WINDOWS SMART HOME EXPLORE SUBSCRIBE

Why You Shouldn't Use SMS for Two-Factor Authentication (and What to Use Instead)



CHRIS HOFFMANN
UPDATED JULY 3, 2017, 12:33PM EDT



TRENDING

Not such a good idea

Session: Short Papers

RESEC'18, June 4, 2018, Incheon, Republic of Korea

<https://dl.acm.org/doi/pdf/10.1145/3203422.3203426>

Cracking IoT Device User Account via Brute-force Attack to SMS Authentication Code

Dong Wang
University of Electronic Science and
Technology of China
jgj212@gmail.com

Jiang Ming
The University of Texas at Arlington
jiang.ming@uta.edu

Ting Chen
University of Electronic Science and
Technology of China
brokendragon@uestc.edu.cn

Xiaosong Zhang*
University of Electronic Science and
Technology of China
johnsonzxs@uestc.edu.cn

Chao Wang
ADLab of Venustech
wangchao3@venustech.com.cn

FORTUNE

RANKINGS ▾

MAGAZINE

NEWSLETTERS

VIDEO

PODCASTS

CONFERENCES

COVID-19

THE 21ST CENTURY CORPORATION • CYBERSECURITY

Time Is Running Out For This Popular Online Security Technique

BY DAVID MEYER

July 26, 2016 4:49 PM GMT+3

<https://fortune.com/2016/07/26/nist-sms-two-factor/>

So Far

- Human Authentication
 - Password basics
 - Multi-factor authentication
 - Password storage
 - Password alternatives

How does the system store them?

- Is the password file readable by the OS?
 - Then if I break the OS...
- Can privileged users see the file?
 - ... and make copies
- Is the file backed up somewhere
 - ... insecure?
- Is the file/password in plaintext somewhere in memory?
 - Core dump or memory scan (Windows)
- Fool the user
 - A program that masquerades as the authentication program
- Similar problems for database Username / Password tables

Counter-hacks

Control-Alt-Del for logging in

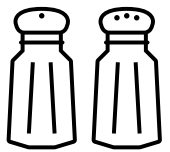
- Establishes a "trusted path" in hardware
- Prevents trojan horses from intercepting passwords

Slow down / restrict number of tries

- Make guessing take too long
- e.g. 3 tries and you're blocked for 30 seconds

Encrypt the password file and hash the passwords

- System admin doesn't know the password!
- Use one way hashes or encryptions on the passwords
- "Salt" - to prevent duplicate passwords showing as duplicate codes

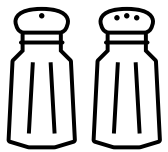


Add Salt

- “Salt” the passwords by adding random bits.
 - Decreases the likelihood that two identical passwords will appear as identical entries in the password file.
- 12 bit salt results in 4,096 versions of each password.
- Unix: `/etc/passwd` entry:

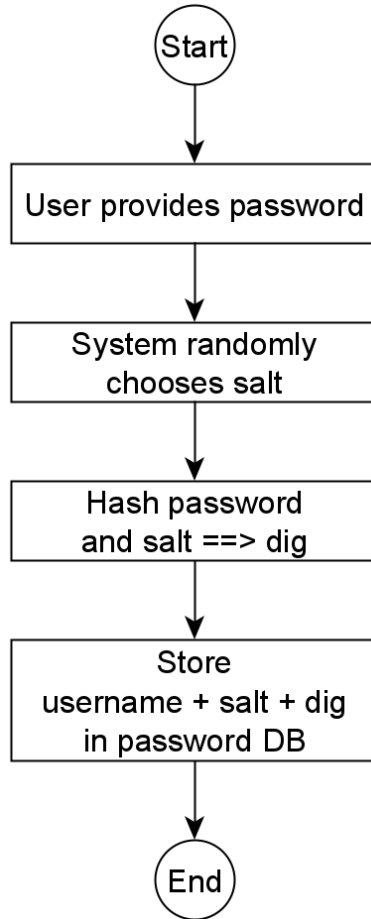
user_id	salt _u	Hash(salt _u + passwd _u)	...
---------	-------------------	--	-----

- Modern implementations of Unix/Linux use so-called *shadow* password files `/etc/shadow` that aren't world readable.
- Most use longer salts now too (48 bits to 128 bits)

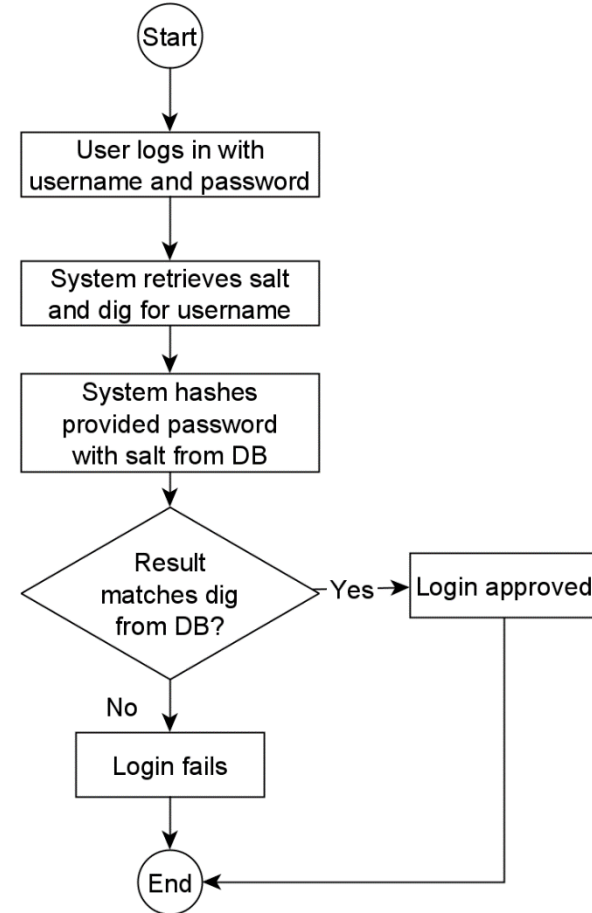


Using Salt

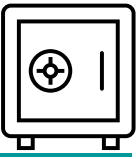
Registration



Login



Password File Hardening



- What if an attacker steals the password file (or database table)?
 - Simple hashes of passwords can be attacked using Rainbow Tables (precomputed hash chains)
- Harden the password file: Make the password + salt → code calculation hard:
 - Old: Encrypt with DES using password and salt 25 times
 - **Newer:** 5,000 rounds of SHA-2 on the password and salt
 - Minimum 1,000 rounds
- More rounds and large salt make Rainbow Tables unfeasible
- Also make guessing attacks longer
- Read more: `crypt()`, PBKDF2, John the Ripper
(<https://www.openwall.com/john/>)



NYTimes Breach Lessons

► SECURITY

The New York Times source code leaked by a 4chan user

An anonymous user has published a torrent file with 270GB worth of data.



by [Alex Ivanovs](#) June 8, 2024

Here are some other findings we can confirm:

- The leak does have the original source code of the game [Wordle](#), which the Times acquired [in 2022](#).
- The leak includes a WordPress database of 1,500 *NY Times Education* site users. The database contains names and surnames, email addresses, and hashed passwords.
- Several folders contain internal communications from Slack channels.
- Many exposed authentication methods exist, including authentication URLs and their respective passwords, secret keys, and API tokens. The majority are well protected, but plenty of such secrets need immediate attention. We have also seen private user keys used for authentication.

<https://stackdiary.com/the-new-york-times-source-code-leaked-by-a-4chan-user/>

Dropbox too

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>

Blog / Product news

A recent security incident involving Dropbox Sign

by Dropbox Sign team

May 1, 2024 • 6 minute read



On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed Dropbox Sign customer information. We believe that this incident was isolated to Dropbox Sign infrastructure, and did not impact any other Dropbox products. We're in the process of reaching out to all users impacted by this incident who need to take action, with step-by-step instructions on how to further protect their data. Our security team also reset users' passwords, logged users out of any devices they had connected to Dropbox Sign, and is coordinating the rotation of all API keys and OAuth tokens. Please read on for additional details and an FAQ.

On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed data including Dropbox Sign customer information such as email addresses, usernames, phone numbers and hashed passwords, in addition to general account settings and certain authentication information such as API keys, OAuth tokens, and multi-factor authentication.

Also a Bank

<https://thecyberexpress.com/alleged-ecb-data-breach-claimed-by-intelbroker/>

[Home](#) » [Firewall Daily](#) » [Dark Web News](#) » 'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)

'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)

The dataset contained various user account information, such as email addresses, hashed passwords, and dates of registration and last login.

by Ashish Khaitan — March 26th, 2024 

Source: xkcd.com



Password Reuse: Problem

2011 Study:

- 49% of users on one site reused the password on a different site
- Makes it worse if the site uses email address as login
- Bad if you use the same user name on multiple sites

2015 Study (Harris Interactive)

- 59% of consumers reuse passwords

2017 Survey (Digital Guardian):

- 60% of consumers reuse passwords

Password Reuse: Problem

- Recent(ish) news:

2 April 2014:

- Ars Technica reports 158,000 passwords from Boxee.tv (Israeli startup) published

15 June 2015:

- LastPass password vault website hacked, password hints, salts, and authentication hashes stolen.

7 Jan 2023:

- Israeli researcher reports leak of 235m email addresses linked to Twitter accounts

From the past year or so

 cybernews®

[Home](#) » [Security](#)

RockYou2024: 10 billion passwords leaked in the largest compilation of all time

Last updated: 4 July 2024  6



Vilnius Petkauskas, Deputy Editor

Issues

VentureBeat



Subscribe

GamesB

e ▾

Security ▾

Data Infrastructure ▾

Automation ▾

Enterprise Analytics ▾

More ▾

Report: Hackers leaked over 721 million passwords in 2022

Tim Keary
[@tim_keary](#)

March 14, 2023 3:00 AM

From the past year or so

If you purchase via links on our site, we may receive **affiliate commissions**.

[Home](#) » [News](#)

Outdated password exposed Poland's military secrets

Updated on: 12 May 2023 





Vilius Petkauskas, Senior Journalist

[Home](#) > [News](#) > [Security](#) > [NortonLifeLock warns that hackers breached Password Manager accounts](#)

NortonLifeLock warns that hackers breached Password Manager accounts

By [Bill Toulas](#)

 January 13, 2023

 11:47 AM

 7

Password Reuse Solutions

Don't use the same login or passwords for multiple websites

Single Sign On systems (OAuth, Kerberos)

Host proof password management tools

Passwordless Future

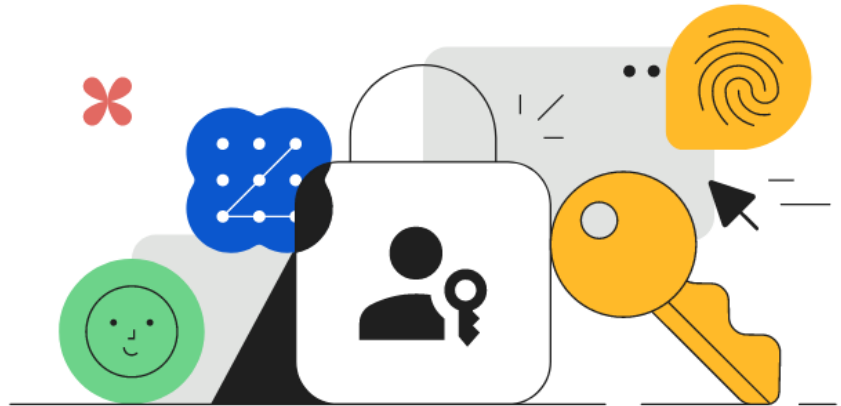
Google Identity

Authentication

The simplest and most secure way to sign in to your Google Account


Passkeys are an easier and more secure alternative to passwords. They let you sign in with just your fingerprint, face scan or screen lock.

[Get passkeys](#)



Facebook Too

Add a security key to your Facebook account

 Copy link

[Computer Help](#)

[iPad App Help](#)

[iPhone App Help](#)

[Android App Help](#)

[More](#) ▼

In order to add a security key to your account, you'll first need to purchase your own third party [Universal 2nd Factor \(U2F\) or FIDO2 security key](#).

Some types of keys can be used by inserting them into a USB or lightning port. Other types of keys can be used by holding them near your computer or mobile device. Before purchasing, make sure that your security key is compatible with the browser and the device that you use to log into your account. After you add a key to your account, you can then use that key to log in.

[Learn more about security keys and how they work.](#)













Microsoft Too

Passwordless authentication

Hackers don't break in—they sign in. Protect one of attackers' most common entry points by going passwordless.

Take sign-in security from better to best

Minimize the threat of password theft for good with the strongest authentication method available in the marketplace.

Bad  Password (Only)	Good  Password +	Better  Password +	Best Passwordless 
123456	 SMS	 Authenticator (Push notifications)	 Windows Hello
qwerty			
password	 Voice	 Software Tokens OTP	 Authenticator (Phone Sign-in)
lloveyou			
Password1		 Hardware Tokens OTP (Preview)	 FIDO2 security key

So Far

- Human Authentication
 - Password basics
 - Multi-factor authentication
 - Password storage
 - Password alternatives



- Finger/Hand print
- Iris
- Cadence (typing, walking)
- Voice print
- Face

- Collection/Enrollment
- Theft
- Ambiguity/Uniqueness
- Accuracy of reader

Biometrics: Fingerprints

- Relatively cheap (\$10 for a simple)
- Can match quickly (2s)
- Data is small (<1KB), so database is small
- Less affected by vandalism/dirt
- Can detect fakes/late

Issues:

- Caucasians have best defined prints
- Women have finer prints
- Manual workers, elderly have less defined prints
- Building trusted path to reader

Technique	Size	Cost	Ease of Use	Dirt Affected	Wear Affected	Easily Duped
Optical	Small	Low	Easy	Yes	Yes	Easy
Capacitance	Small	V. Low	Easy	Yes	Yes	Easy
RF	Small	V. Low	Easy	No	No	Difficult
Ultrasound	V. Large	V. High	Easy	No	Yes	Medium
Thermal	V.Small	Low	Difficult	Yes	Yes	Medium
Pressure	Small	V. Low	Easy	Yes	Yes	Medium

Reference: Coventry "Fingerprint Authentication". (2004)

Other Biometrics

Voice print: Speak a fixed statement prerecorded

- Issues:
 - High quality recordings of voice
 - Problems with voice – cold, cough, etc.

Retinal scans: Picture of back of eye

- Very high quality
- Issues:
 - Physical proximity
 - Relatively long scan time (15s)

Iris scans: Scans iris pattern into a barcode

- Similar to retinal scan, but not as accurate

Facial recognition: Measure facial geometry

- Medium quality authentication
- Issues:
 - Masks, hats, bandages on face, facial hair
 - Reference: Alexander and Smith. “Engineering Privacy in Public: Confounding Face Recognition”. 2003

AI complicates voice

The screenshot displays the ElevenLabs website. At the top, the navigation bar includes the ElevenLabs logo, links for Products, Research, Pricing, Resources, and Enterprise, and a Sign In button. The main content area features a large heading 'AI Voice Cloning: Clone Your Voice in Minutes' and a subtext describing the service's accuracy and availability. A yellow button labeled 'Clone Your Voice' is positioned below the text. To the right, three rows of audio player controls are shown, each comparing an 'Original' voice sample with an 'AI' generated sample for characters named Glinda, James, and Tiffany. Each sample is accompanied by a play button icon and a small colored label indicating the character's name.

ElevenLabs Products ▾ Research ▾ Pricing Resources ▾ Enterprise ▾ Sign In

AI Voice Cloning: Clone Your Voice in Minutes

Create your AI voice clone from just a few minutes of audio. Reach unparalleled accuracy across 29 languages and 50+ accents. ElevenLabs Voice Cloning is the most advanced voice cloning AI available.

[Clone Your Voice →](#)

Original Glinda

AI Glinda

Original James

AI James

Original Tiffany

AI Tiffany

AI complicates facial recognition

IEEE Spectrum Hackers Compete to Confound Facial Recognition

Q Type to search

NEWS ARTIFICIAL INTELLIGENCE

Hackers Compete to Confound Facial Recognition

› Def Con challenge organizers hope to spur better security in the industry

BY EDD GENT | 29 AUG 2022 | 3 MIN READ |



<https://spectrum.ieee.org/facial-recognition>

The real Brad Pitt (L) versus an AI Brad Pitt (R). LEFT: MATT SAYLES/AP; RIGHT: DEFCON

Conclusion

- Human Authentication
 - Password basics
 - Multi-factor authentication
 - Password storage
 - Password alternatives