The Password Doesn’t Fall Far: How Service Influences Password Choice

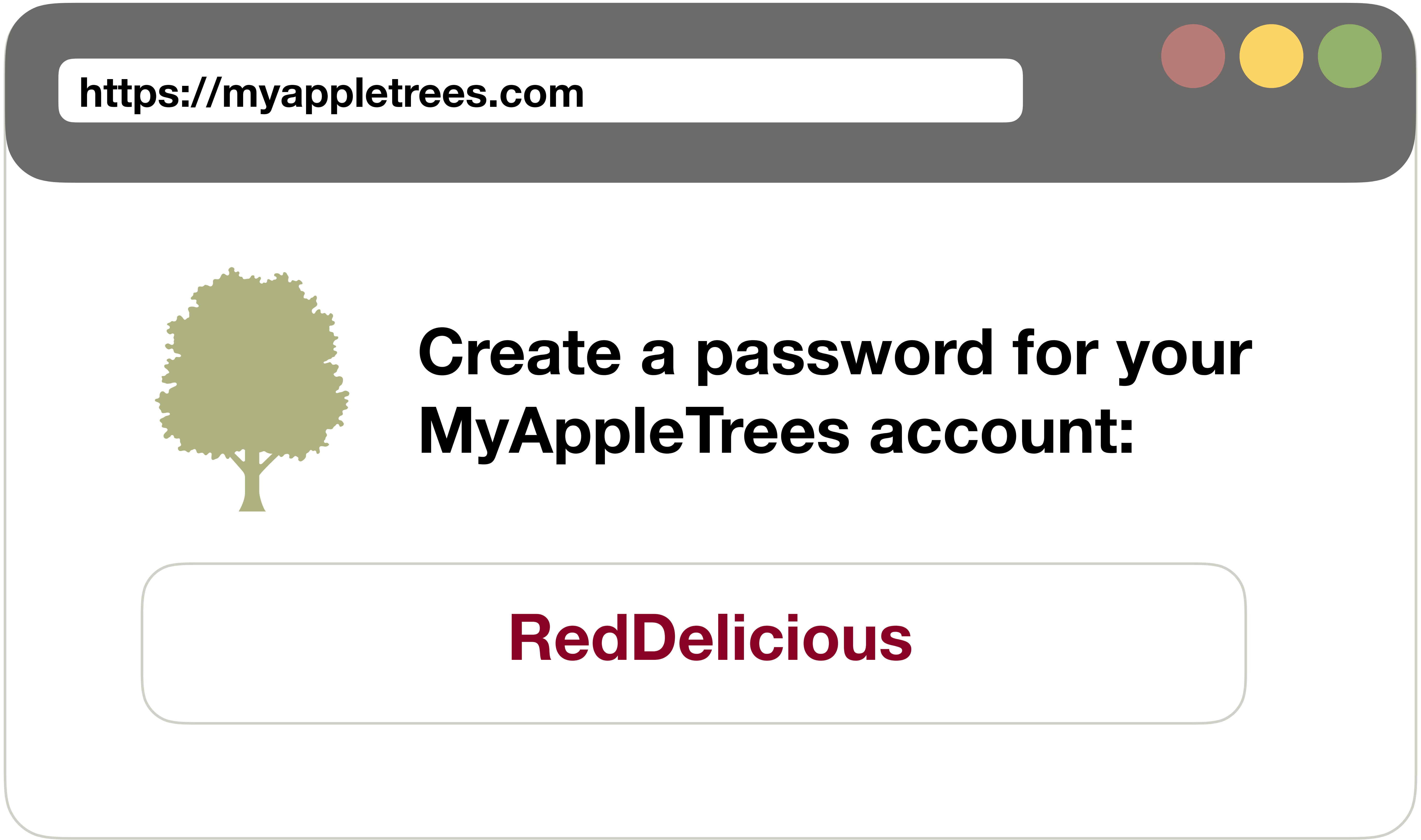
Miranda Wei, The University of Chicago
Maximilian Golla, Ruhr University Bochum
Blase Ur, The University of Chicago

Baltimore, USA | August 12, 2018

https://myappletrees.com

Create a password for your MyAppleTrees account:

MyAppleTreesPassword



https://myappletrees.com

Create a password for your MyAppleTrees account:

RedDelicious

related work about password choice

account importance

[Ur et al., SOUPS15]

composition policies

[Florêncio & Herley, WWW07]

demographic factors

[Mazurek et al., CCS13]

our research questions

Do users make passwords related to…

1. … the name of the service? `myappletrees`
2. … the topic of the service? `applepie`

methodology

five password leaks

BATTLEFIELD heroes™

last.fm

mate1
find someone TODAY

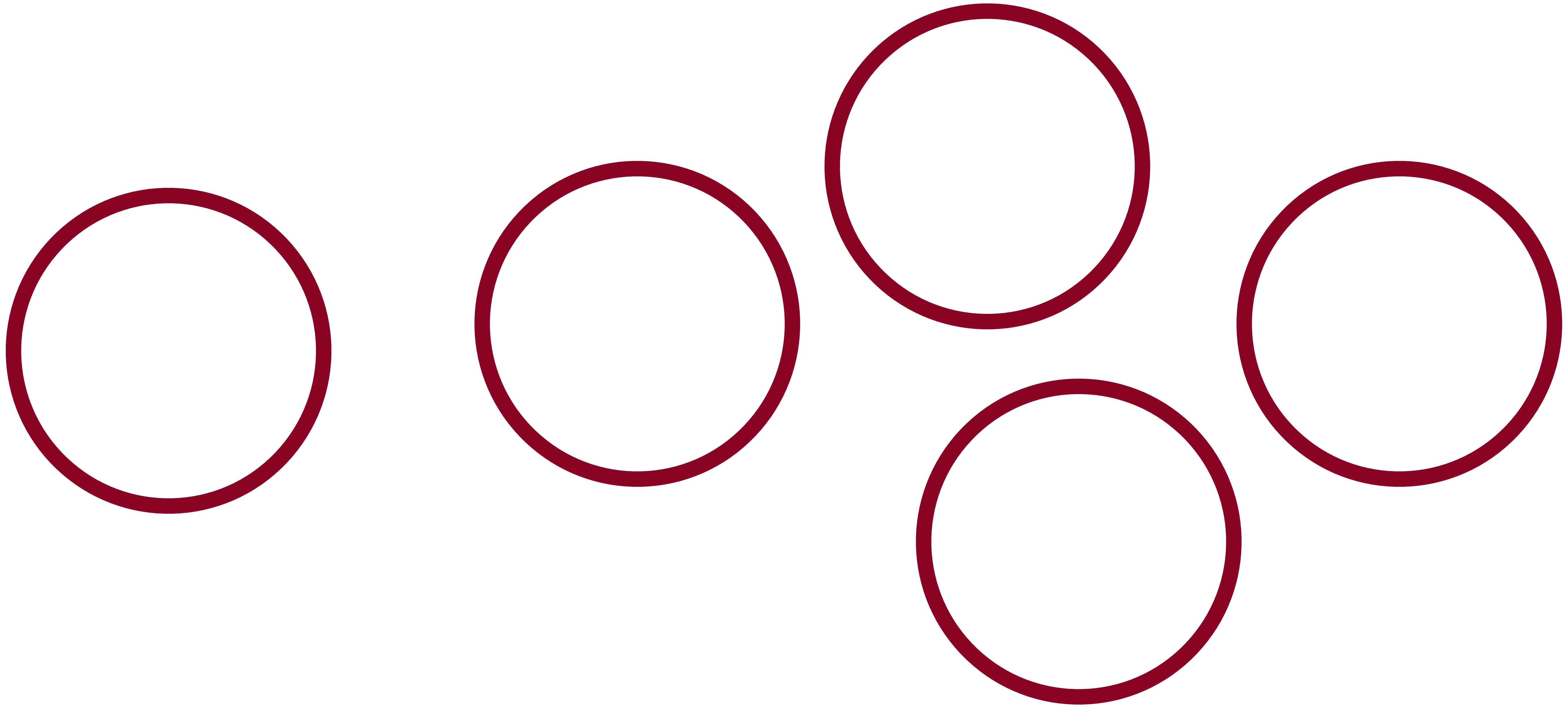
BRAZZERS

LinkedIn

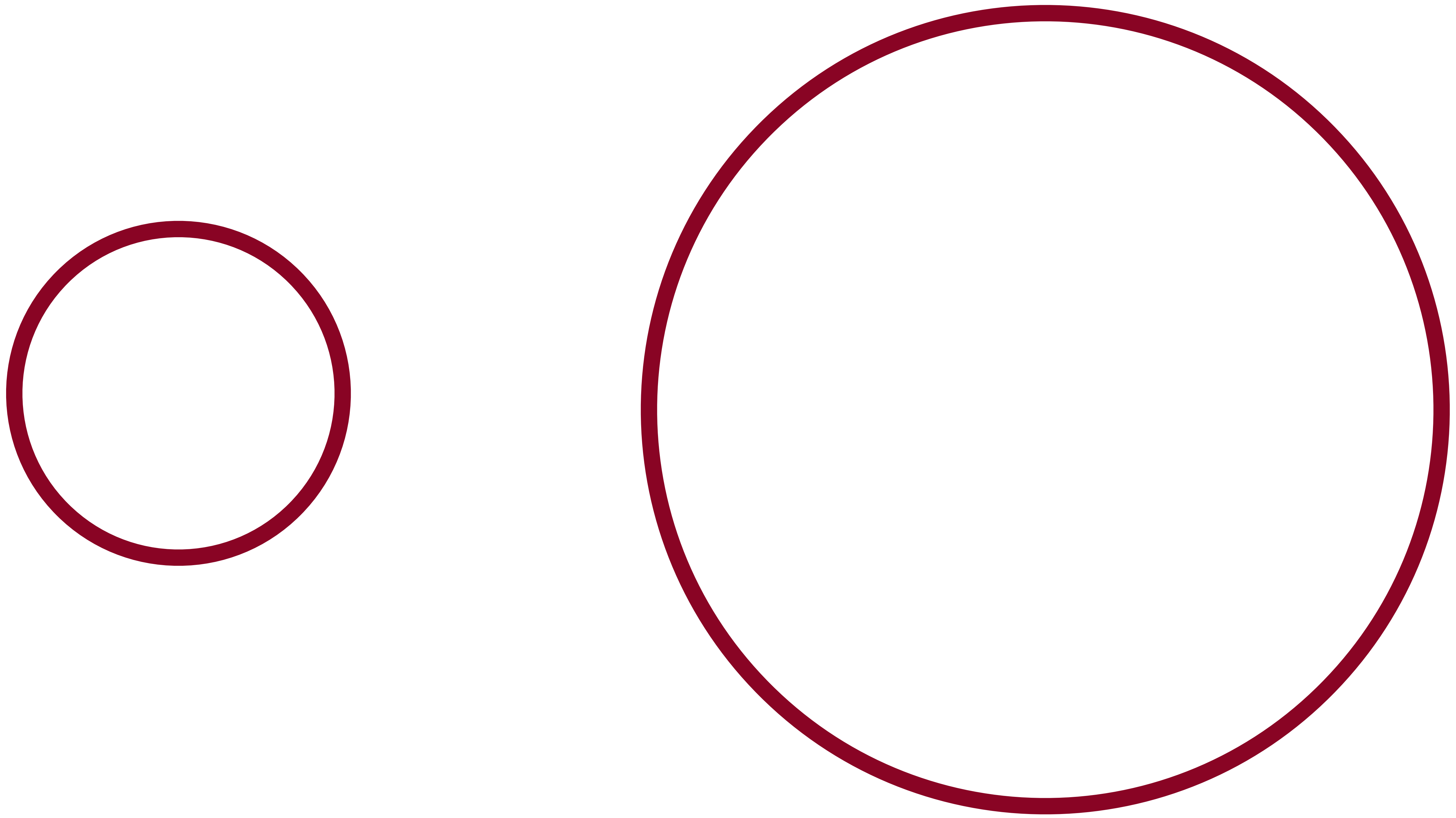
filtered out passwords that appeared in other leaks

Top 1000 Passwords From Battlefield Heroes

Top 1000 Passwords From Each of the Other Four Leaks



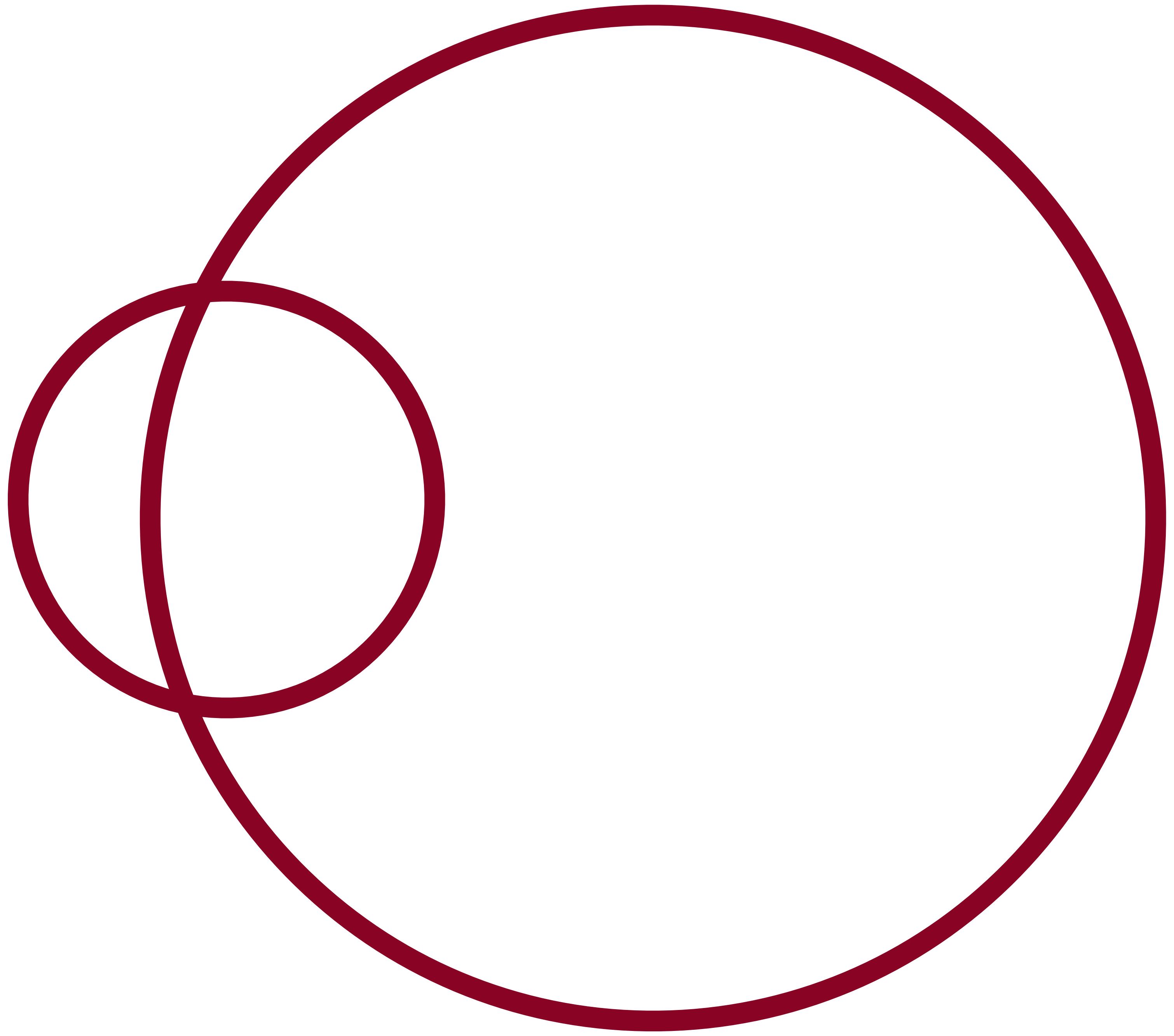
filtered out passwords that appeared in other leaks



Top 1000 Passwords From Battlefield Heroes

Top 1000 Passwords From Each of the Other Four Leaks

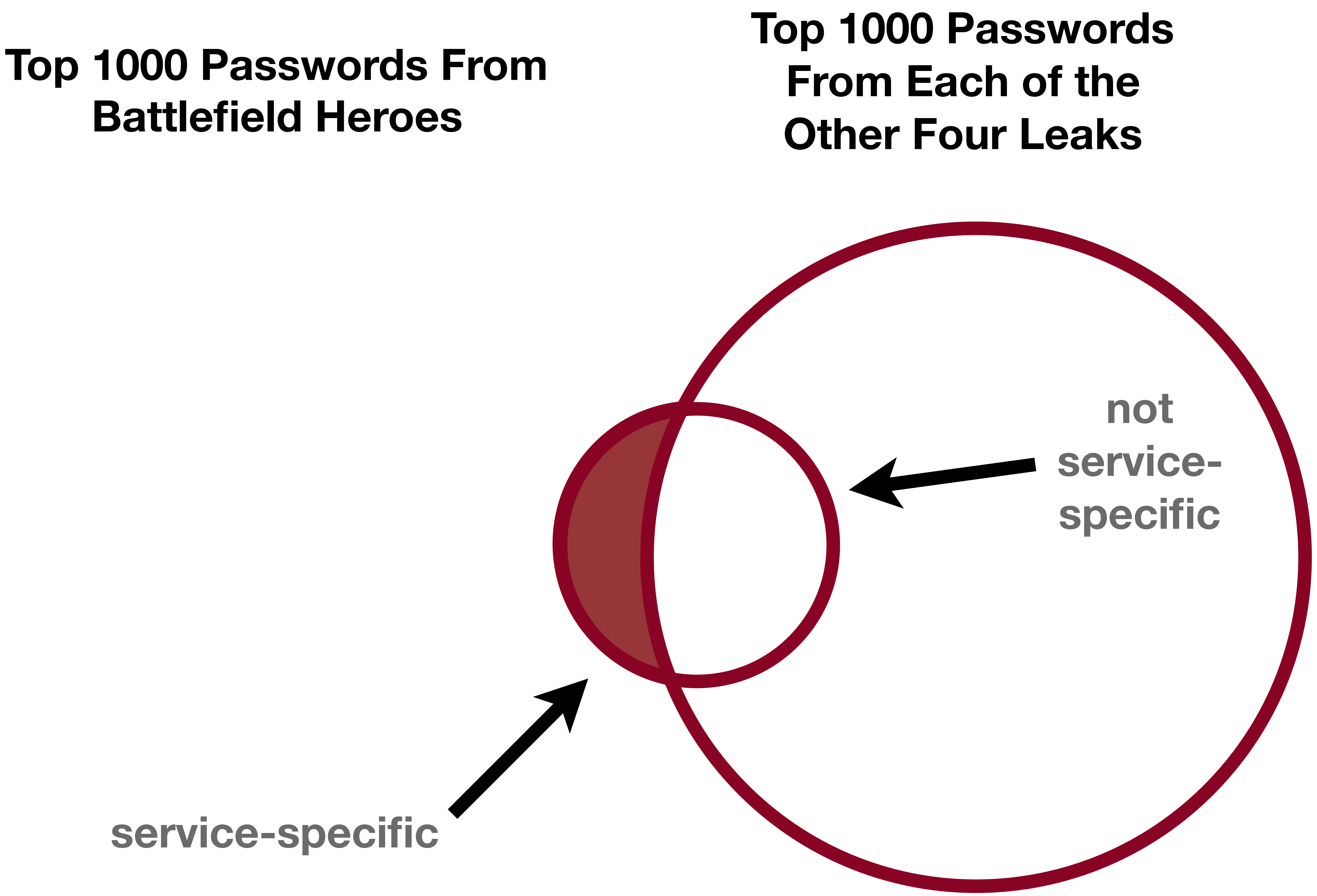
filtered out passwords that appeared in other leaks



Top 1000 Passwords From Battlefield Heroes

Top 1000 Passwords From Each of the Other Four Leaks

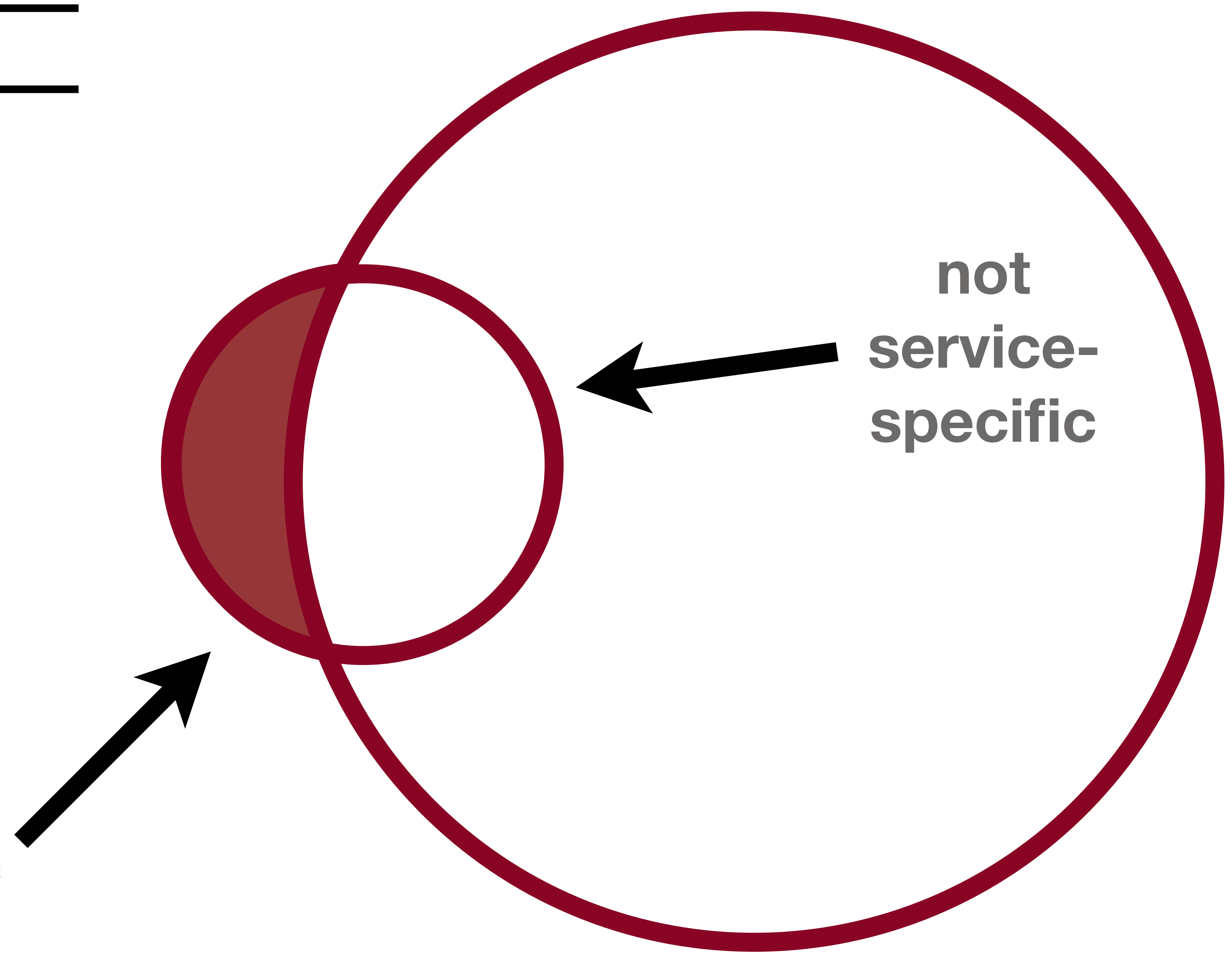
filtered out passwords that appeared in other leaks


Top 1000 Passwords From Battlefield Heroes
Top 1000 Passwords From Each of the Other Four Leaks
not service-specific
service-specific

filtered out passwords that appeared in other leaks

Top 1000 Passwords From
~~Battlefield Heroes~~
~~Brazzers~~
~~last.fm~~
~~LinkedIn~~
Mate1

Top 1000 Passwords From Each of the Other Four Leaks



not service-specific

service-specific

qualitative coding

Step 1: Initial Criteria

Is the password related to…

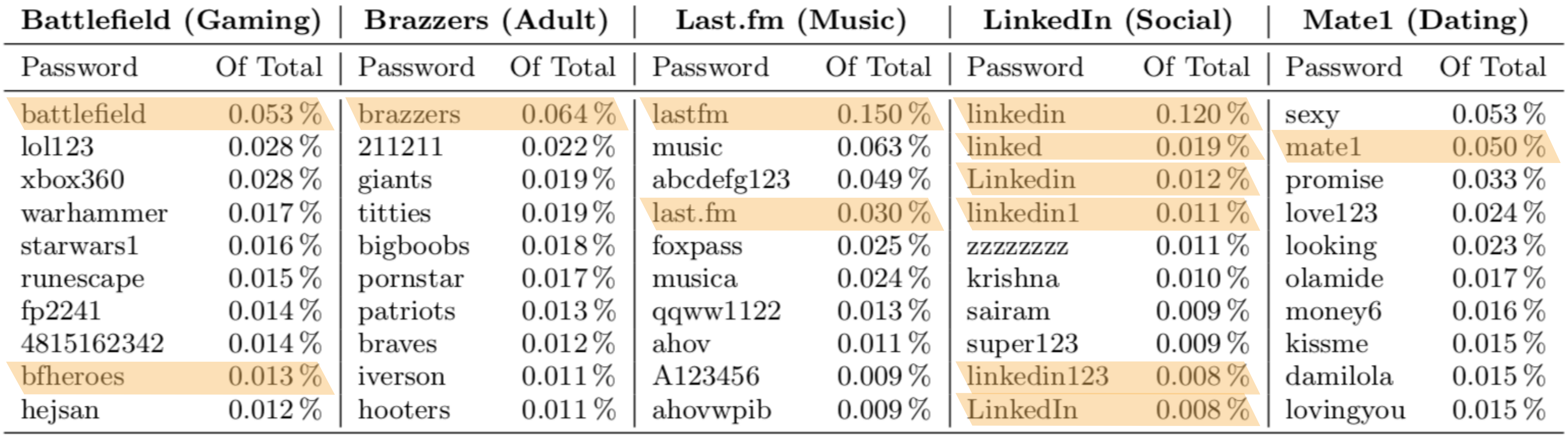
- … the name of the service?
- … the topic of the service?

Step 2: Open Coding

- average of 7 codes/service
- coded 90% of analyzed passwords

results

yes, related to name



Battlefield (Gaming)		Brazzers (Adult)		Last.fm (Music)		LinkedIn (Social)		Mate1 (Dating)	
Password	Of Total	Password	Of Total	Password	Of Total	Password	Of Total	Password	Of Total
battlefield	0.053 %	brazzers	0.064 %	lastfm	0.150 %	linkedin	0.120 %	sexy	0.053 %
lol123	0.028 %	211211	0.022 %	music	0.063 %	linked	0.019 %	mate1	0.050 %
xbox360	0.028 %	giants	0.019 %	abcdefg123	0.049 %	Linkedin	0.012 %	promise	0.033 %
warhammer	0.017 %	titties	0.019 %	last.fm	0.030 %	linkedin1	0.011 %	love123	0.024 %
starwars1	0.016 %	bigboobs	0.018 %	foxpass	0.025 %	zzzzzzzz	0.011 %	looking	0.023 %
runescape	0.015 %	pornstar	0.017 %	musica	0.024 %	krishna	0.010 %	olamide	0.017 %
fp2241	0.014 %	patriots	0.013 %	qqww1122	0.013 %	sairam	0.009 %	money6	0.016 %
4815162342	0.014 %	braves	0.012 %	ahov	0.011 %	super123	0.009 %	kissme	0.015 %
bfheroes	0.013 %	iverson	0.011 %	A123456	0.009 %	linkedin123	0.008 %	damilola	0.015 %
hejsan	0.012 %	hooters	0.011 %	ahovwpib	0.009 %	LinkedIn	0.008 %	lovingyou	0.015 %

Top ten passwords per service after filtering

yes, related to topic

BATTLEFIELD heroes™

trooper

headshot

iamthebest

BRAZZERS

pornstar

enjoyporn

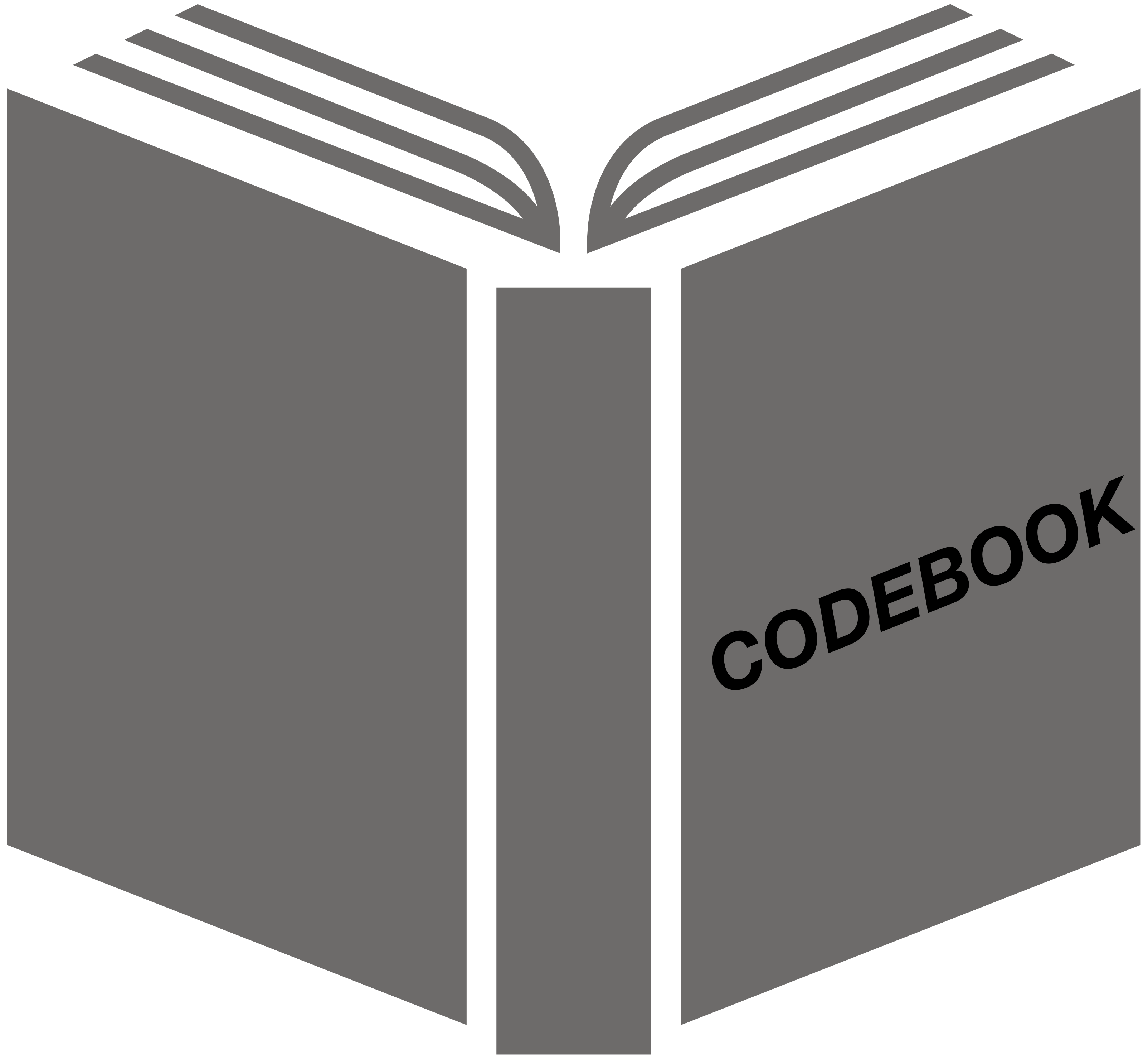
iloveporn

Linkedin

networking

jobsearch

business


CODEBOOK

users choose passwords based on other interests

BATTLEFIELD heroes

🎮

halflife

warcraft3

gamecube

viewsonic

BRAZZERS

⚽

giants

patriots

wrestling

bowling

🛻

cadillac

silverado

peterbilt

accord

users choose passwords reflecting international backgrounds

BATTLEFIELD heroes™

hejhej

jemoeder

wachtwoord

panzer

mate1 find someone TODAY

olamide

opeyemi

babatunde

adekunle

users invoke religion
when it comes to jobs and love

LinkedIn

krishna

jesuschrist

godisgreat

godislove

mate1
find someone TODAY

ilovegod

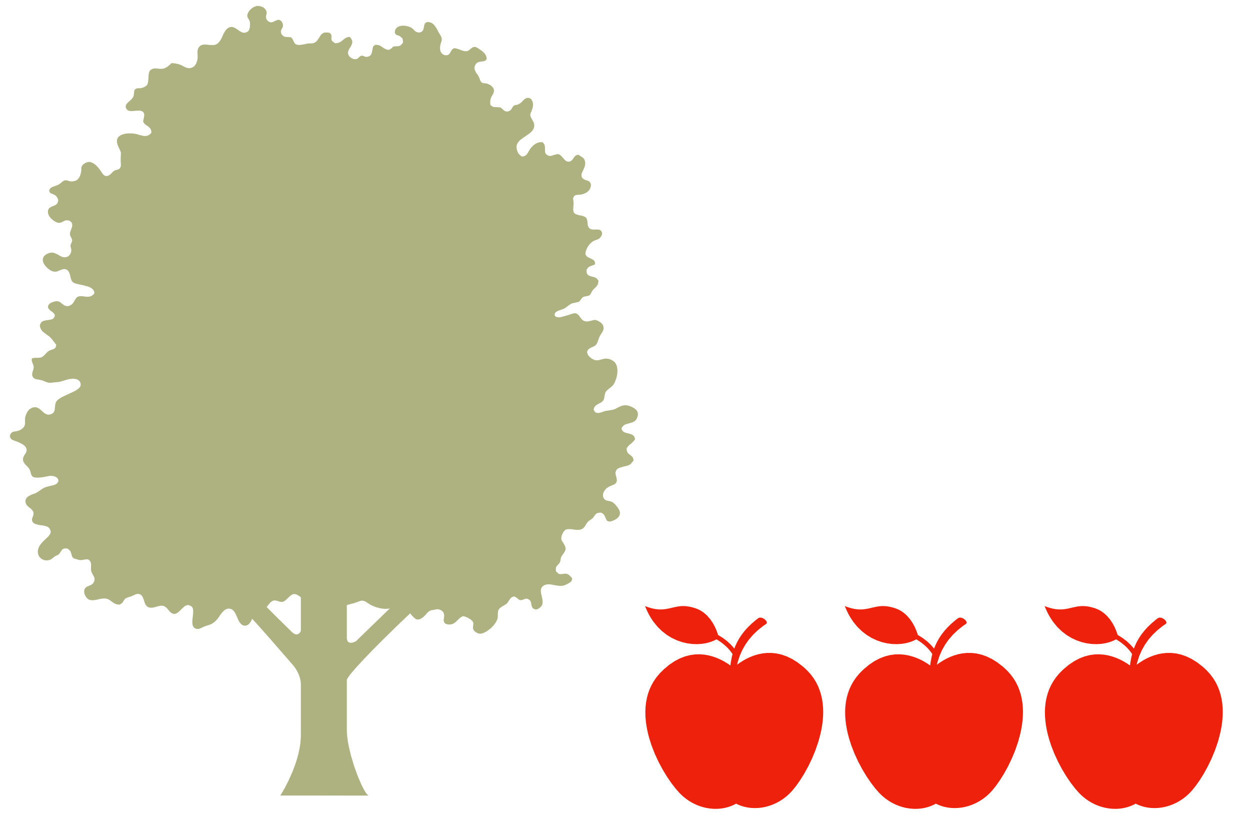
thankgod

ingodwetrust

godhelpme

conclusions

need to account for site-specific keywords

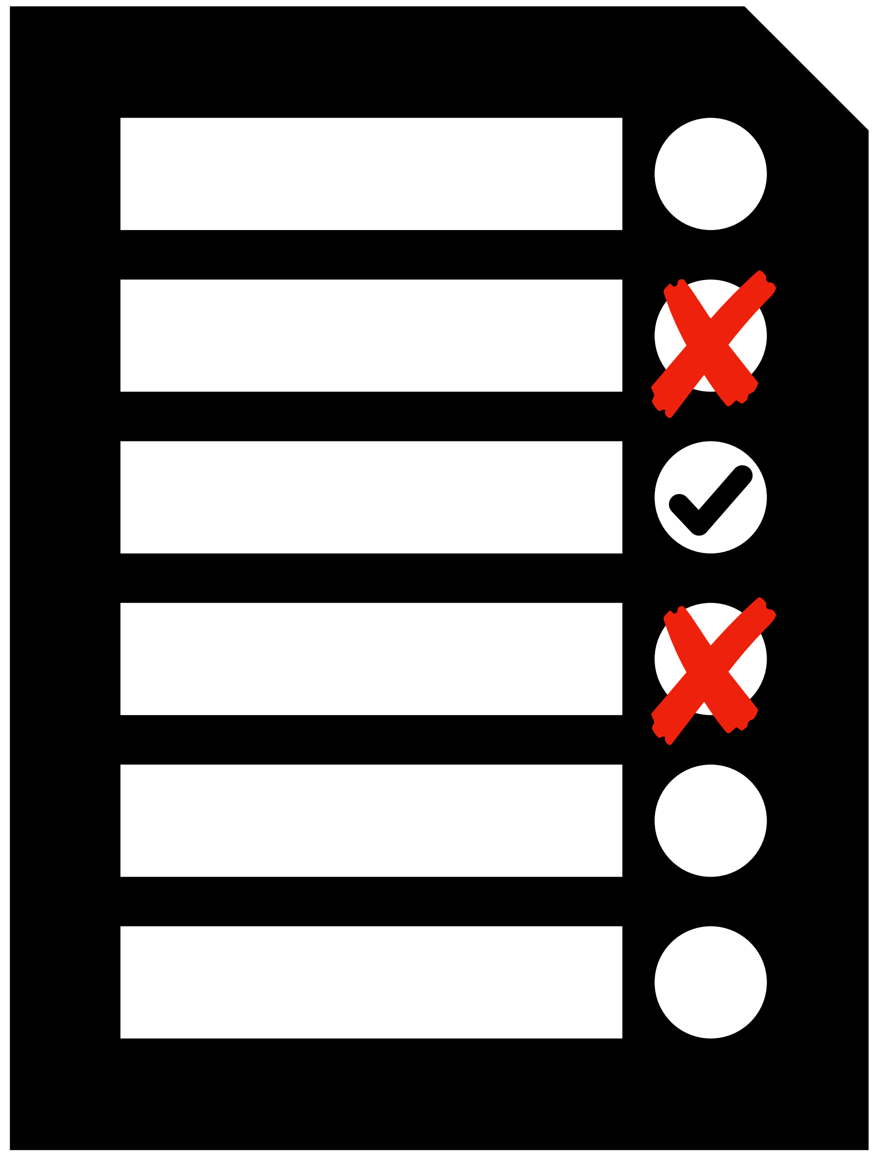


- password doesn't fall far
  - 3-6% of passwords analyzed were directly related to name/topic
- many password-guessing tools/models support custom wordlists

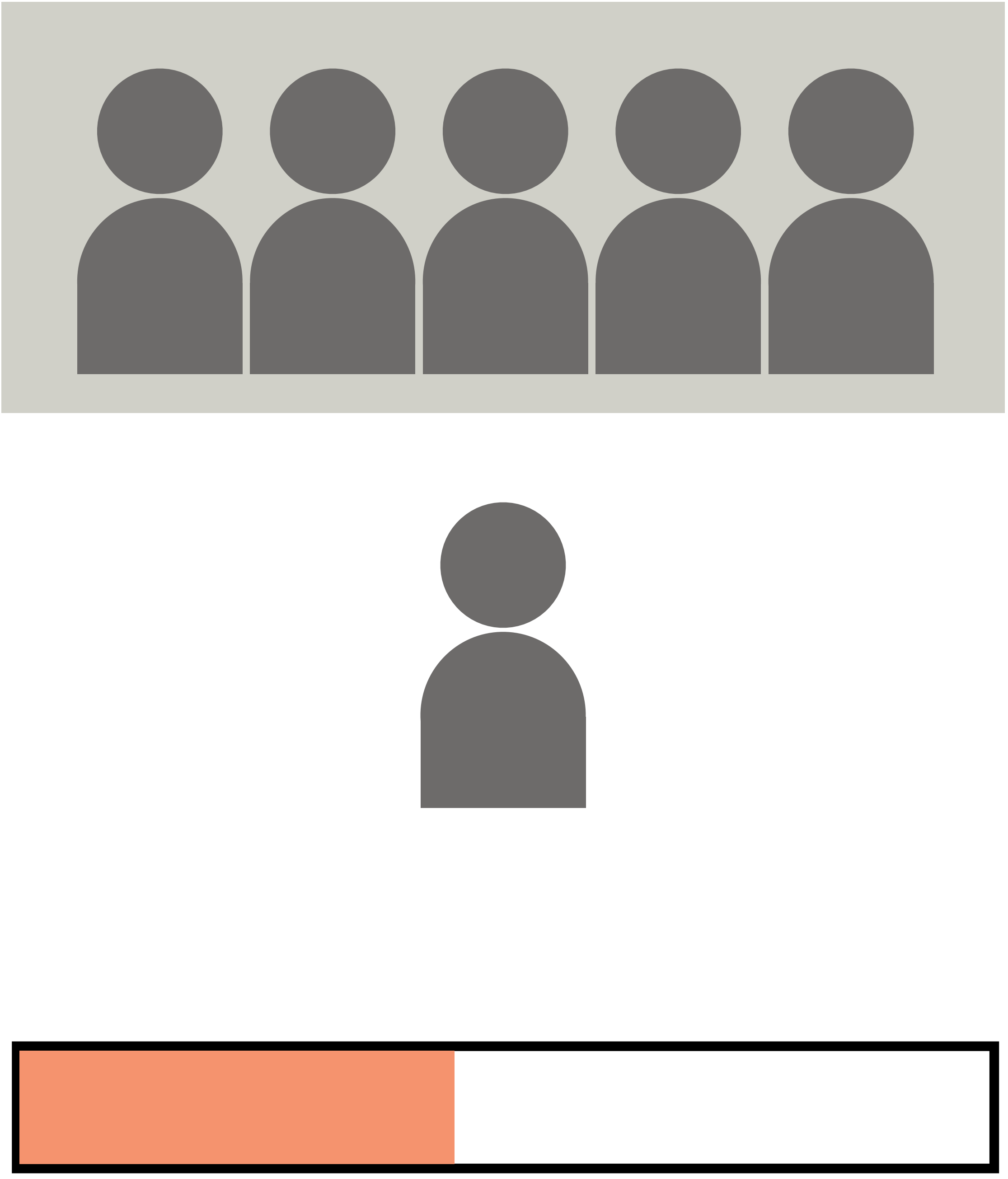
use blacklists

- at an absolute minimum, blacklist the service name!
  - **looking at you:** Spotify, Amazon, Facebook, Google, Hulu, Tumblr, Pinterest, Microsoft, Instagram, Twitter

- balancing security and usability



improve existing tools



- popularity-based password-composition policies

  [Schechter et al., Hot Topics 10, Segreti et al., SOUPS17]

- password-strength meters [Ur et al., CHI17]

- Qualitative study of leaked passwords from Battlefield Heroes, Brazzers, last.fm, LinkedIn, and Mate1
- Passwords were related by service name, topic, and a variety of other salient semantic topics
- Need to account for site-specific keywords

The Password Doesn’t Fall Far: How Services Influence Password Choice

Miranda Wei, Maximilian Golla, Blase Ur
weim@uchicago.edu

title image:
http://www.fanpop.com/clubs/autumn/images/35580383/title/apple-orchard-photo