User Authentication - 1

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

21/01/2025

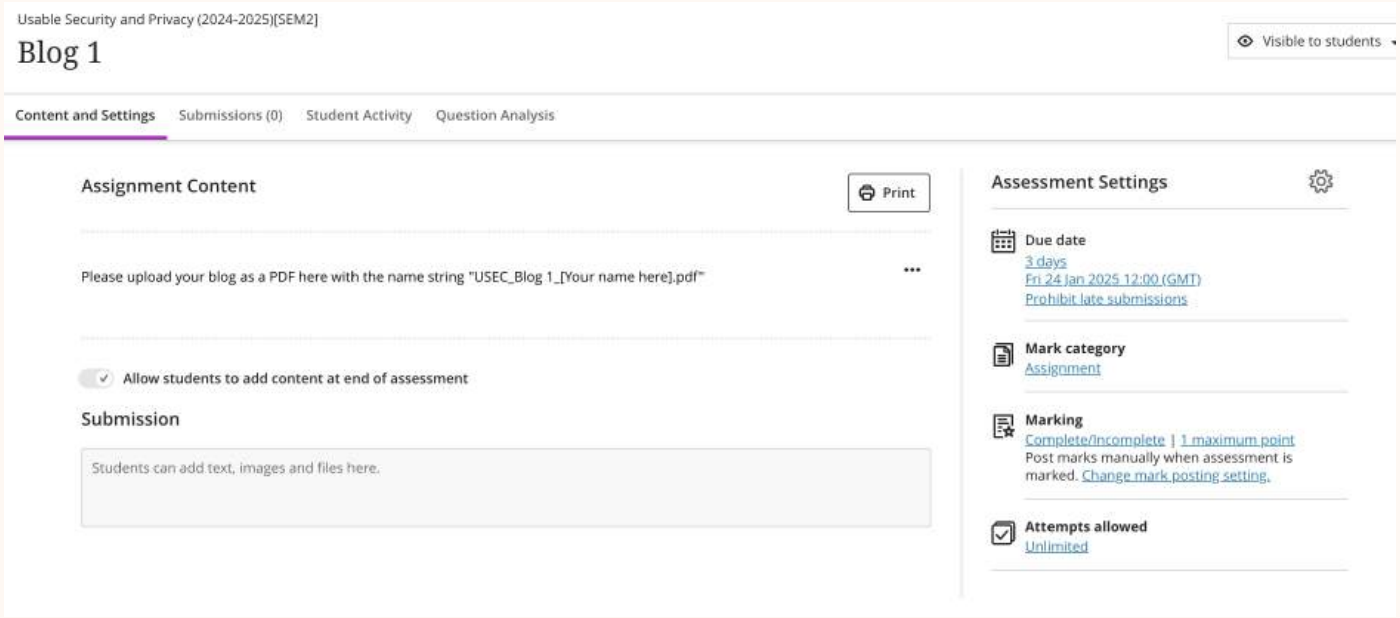
THE UNIVERSITY *of* EDINBURGH

Overview

- Reminder, warm-up, and recap
- Authentication and password
- Take-home

Reminder

- First blog due this Friday on Learn
  - Choose any 1 recommended blog material or related material to reflect on



Gap in security literacy and behavior

"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices

Iulia Ion
Google
iuliaion@google.com

Rob Reeder
Google
rreeder@google.com

Sunny Consolvo
Google
sconsolvo@google.com

ABSTRACT

The state of advice given to people today on how to stay safe online has plenty of room for improvement. Too many things are asked of them, which may be unrealistic, time consuming, or not really worth the effort. To improve the security advice, our community must find out what practices people use and what recommendations, if messaged well, are likely to bring the highest benefit while being realistic to ask of people. In this paper, we present the results of a study which aims to identify which practices people do that they consider most important at protecting their security online. We compare self-reported security practices of non-experts to those of security experts (i.e., participants who reported having five or more years of experience working in computer security). We report on the results of two online surveys—one with 231 security experts and one with 294 MTurk participants—on what the practices and attitudes of each group are. Our findings show a discrepancy between the security practices that experts and non-experts report taking. For instance, while experts most frequently report installing software updates, using two-factor authentication and using a password manager to stay safe online, non-experts report using antivirus software, visiting only known websites, and changing passwords frequently.

1. INTRODUCTION

Frightening stories about cybersecurity incidents abound. The carefully considering the most worth-while advice to recommend is imperative. Even if users accept some responsibility for protecting their data [23, 43] and want to put in some effort [41], we should be thoughtful about what we ask them to do [20] and only offer advice that is effective and realistic to be followed.

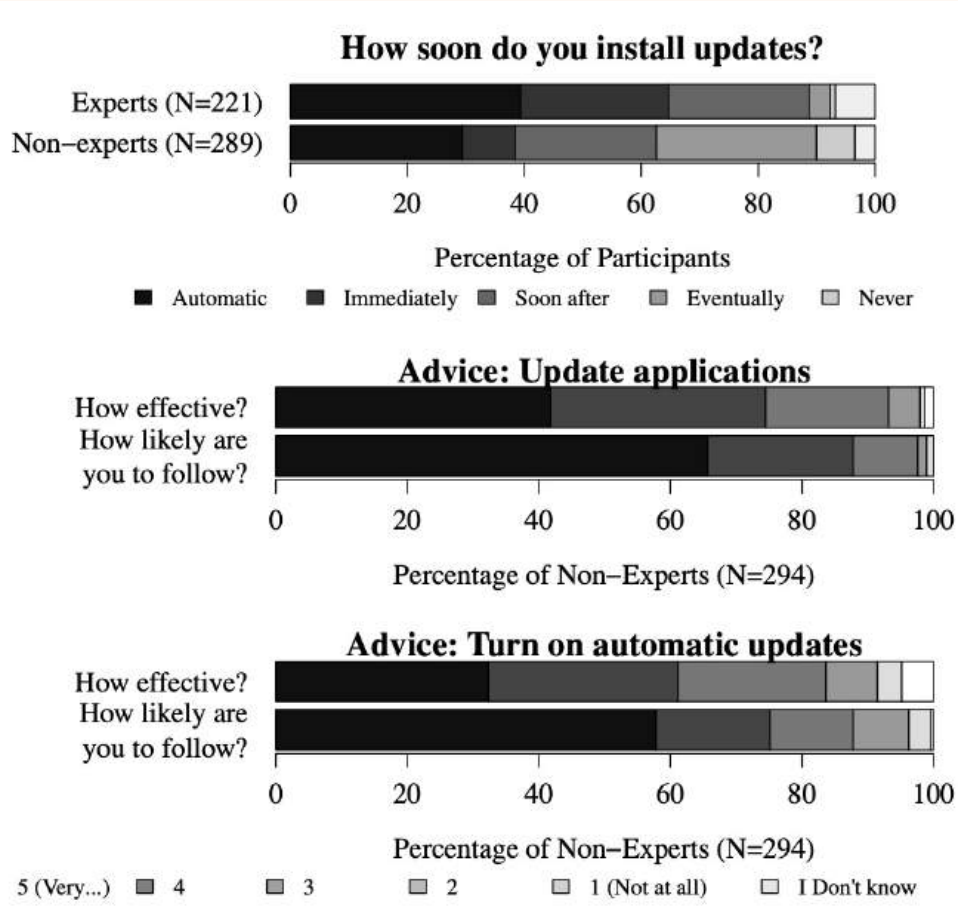
Existing literature on giving good advice suggests that for recipients to follow it, the advice should be (a) useful, comprehensible and relevant, (b) effective at addressing the problem, (c) likely to be accomplished by the recipient, and (d) not possess too many limitations and drawbacks [34]. Therefore, to improve the state of security advice, we must assess which actions are most likely to be effective at protecting users, understand what users are likely and willing to do, and identify the potential challenges or inconveniences caused by following the advice. Furthermore, lessons from health advice in outreach interventions suggest that people will not initiate certain actions if they do not believe them to be effective [53]. Therefore, to learn how to best deliver the advice to users, we must also understand how users perceive its effectiveness and limitations.

In preliminary work, we surveyed security experts to identify what advice they would give non-tech-savvy users. The most frequently given pieces of advice were, in order of frequency: (1) keep systems and software up-to-date, (2) use unique passwords, (3) use strong passwords, (4) use two-factor authentication, (5) use antivirus software, and (6) use a password manager. In this paper, we report on results of a study which tries to identify what security

Gap in security literacy and behavior

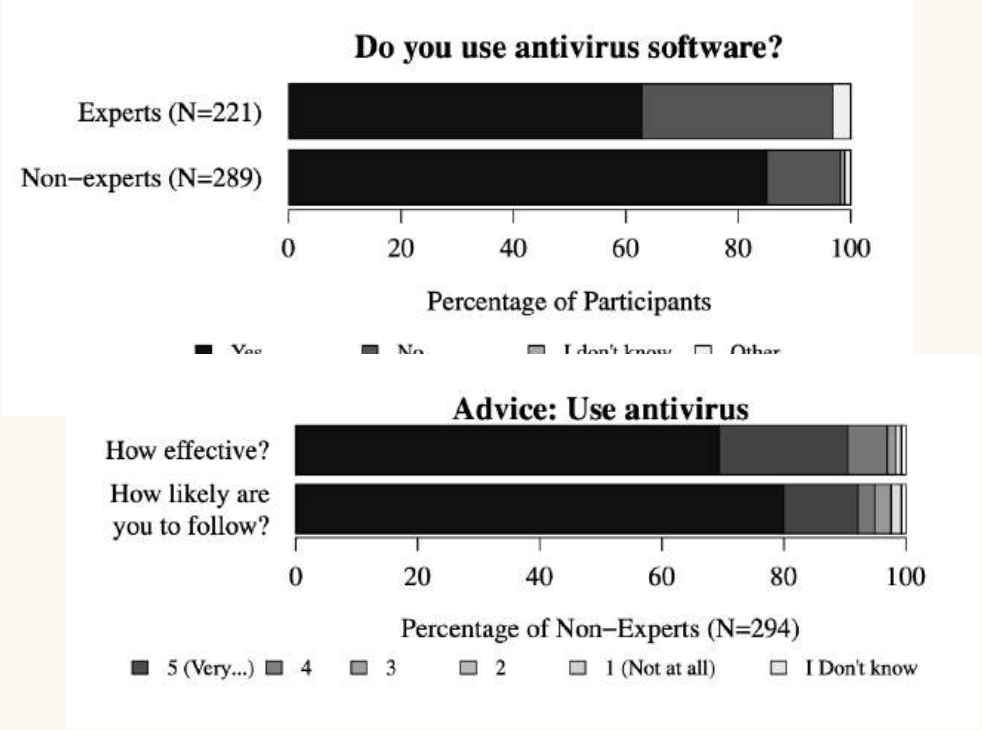
- Types of security behaviors
  - Security updates
    - Bundled with undesirable features; not sure about the benefits of it...
  - Antivirus software
    - Whether people install and how they configure it
  - Account security
    - Password use...
  - Mindfulness
    - Website visits; email habits; phishing notices...

Gap in security literacy and behavior



- Non-experts consider installing security updates not effective, but they will likely to follow if they heard it was effective

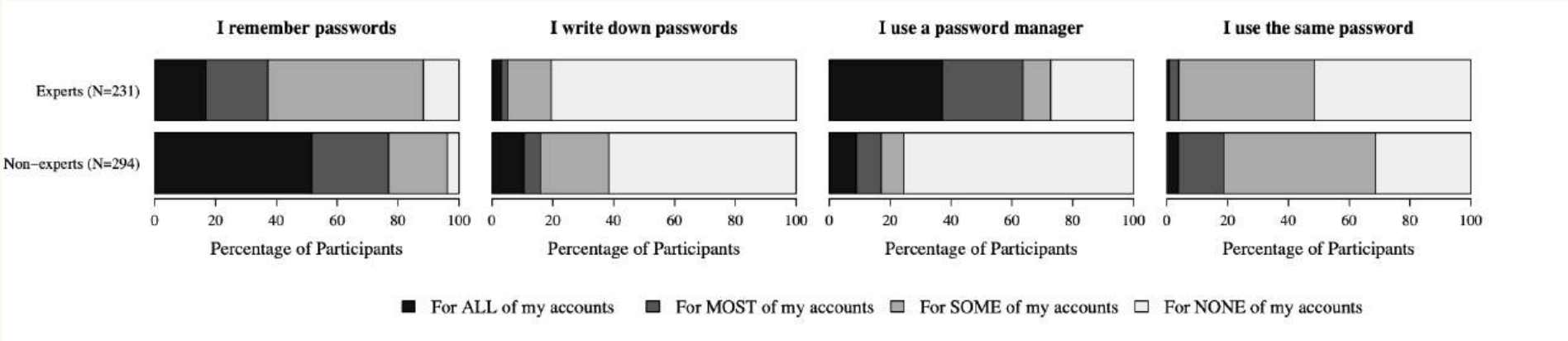
Gap in security literacy and behavior



- More non-experts use anti-virus software than experts and consider it very effective – likely because it is a one-stop solution for them

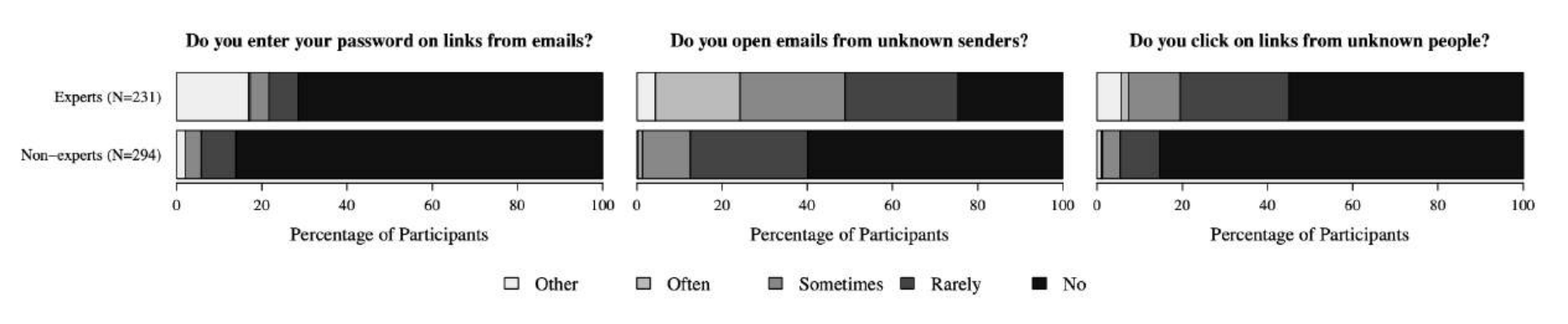
Is it still true today?

Gap in security literacy and behavior



- More experts mention *strong password,* using *password manager, and two-factor authentication*; more non-experts mention using unique password and changing password frequently
- Only one expert mentions writing down passwords is fundamentally bad

Gap in security literacy and behavior



- Paradoxically, more experts clicks on links from unknown senders than non-experts **Why?**
- Other mindfulness aspects include checking HTTPS, clearing browser cookies, and email habits.

https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html

10

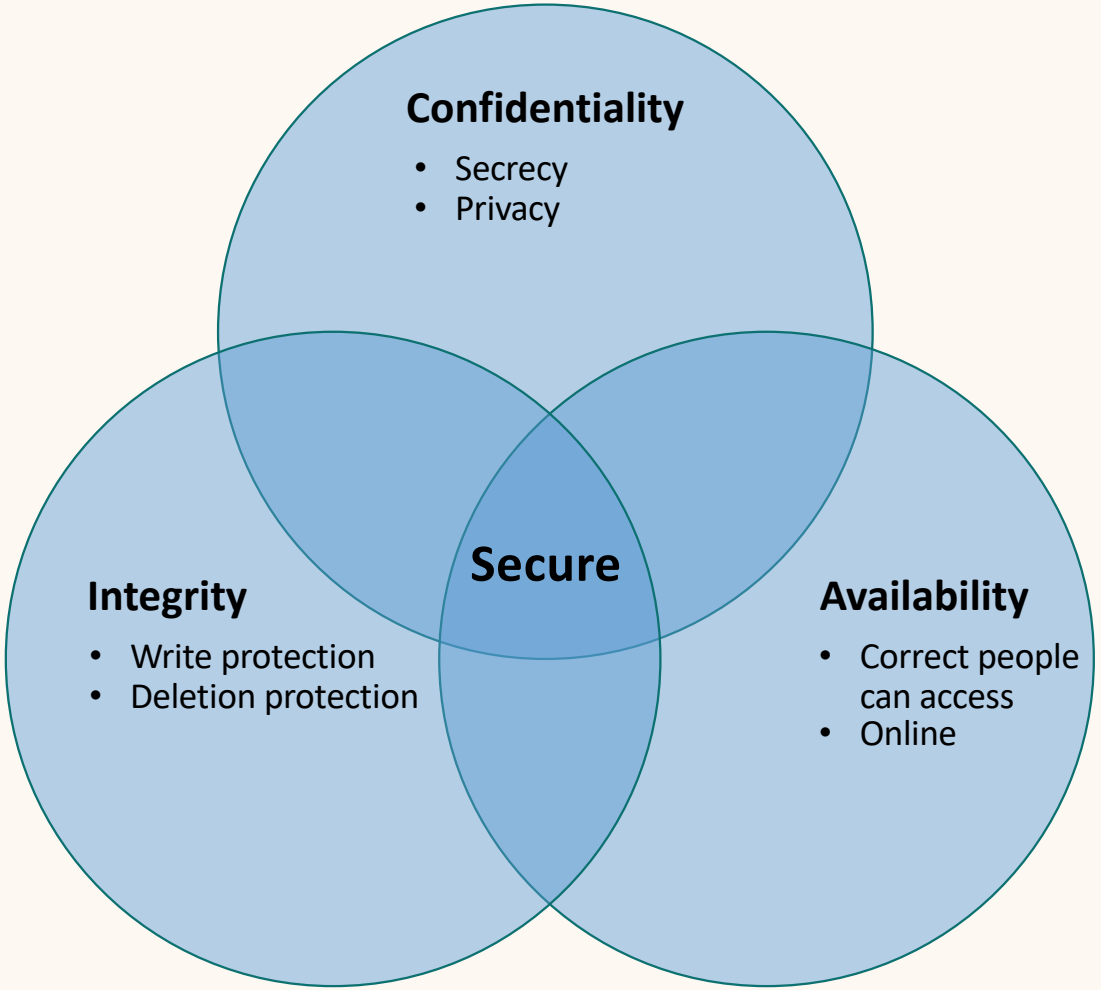
Zoombombing

- BBC - Black and LGBT Edinburgh University students attacked in Zoom meeting (https://www.bbc.co.uk/news/technology-56100079)
- CNN - NYC classrooms cancel Zoom after trolls make ‘Zoombombing’ a thing (https://thenextweb.com/news/nyc-classrooms-cancel-zoom-after-trolls-make-zoombombing-a-thing)

How do we prevent zoombombing from happening?

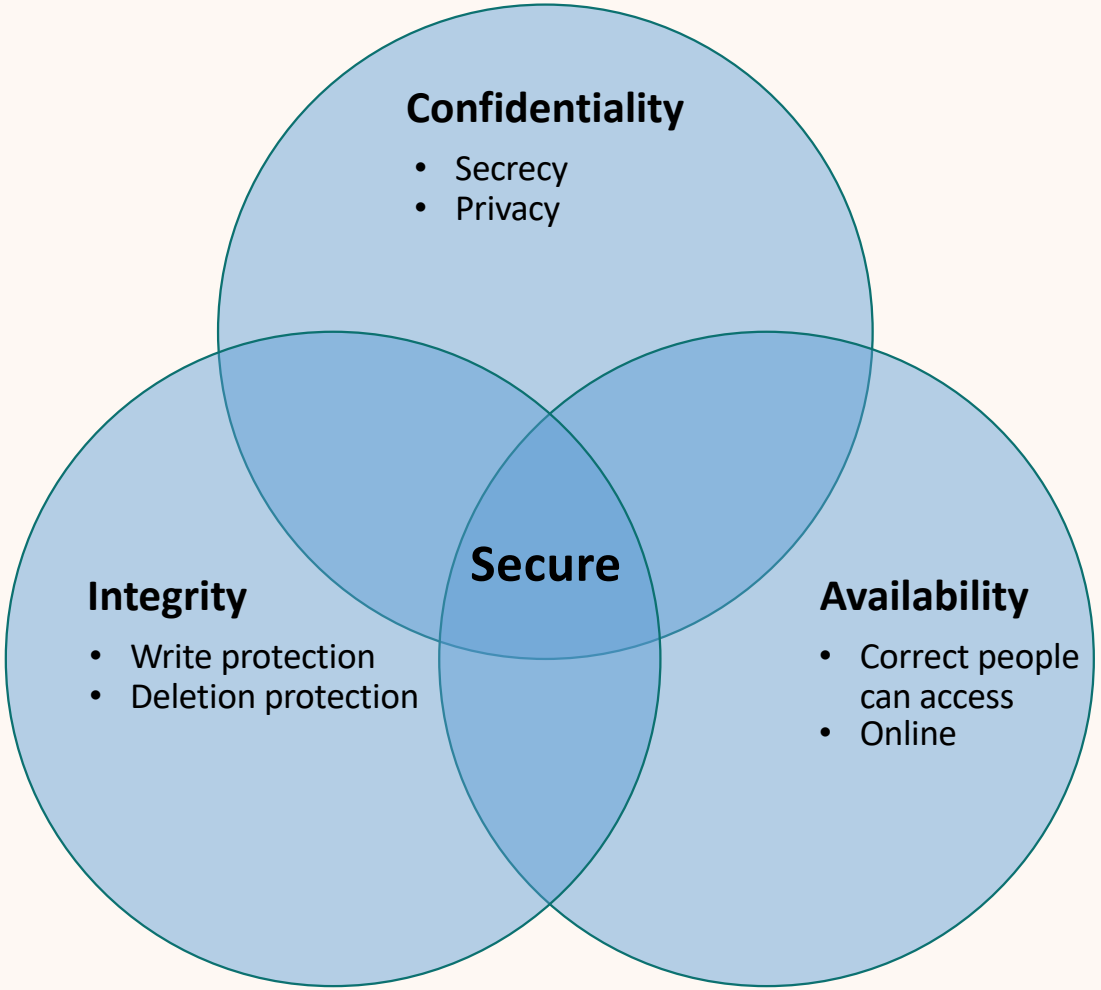
Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.



Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by **authorized** parties.
- Integrity
  - Assets can be modified only by **authorized** parties or only in **authorized** ways.
- Availability
  - Assets are accessible to **authorized** parties at appropriate times.



Cyber Security (CIA)

Security properties	
Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired

Cyber Security (CIA)

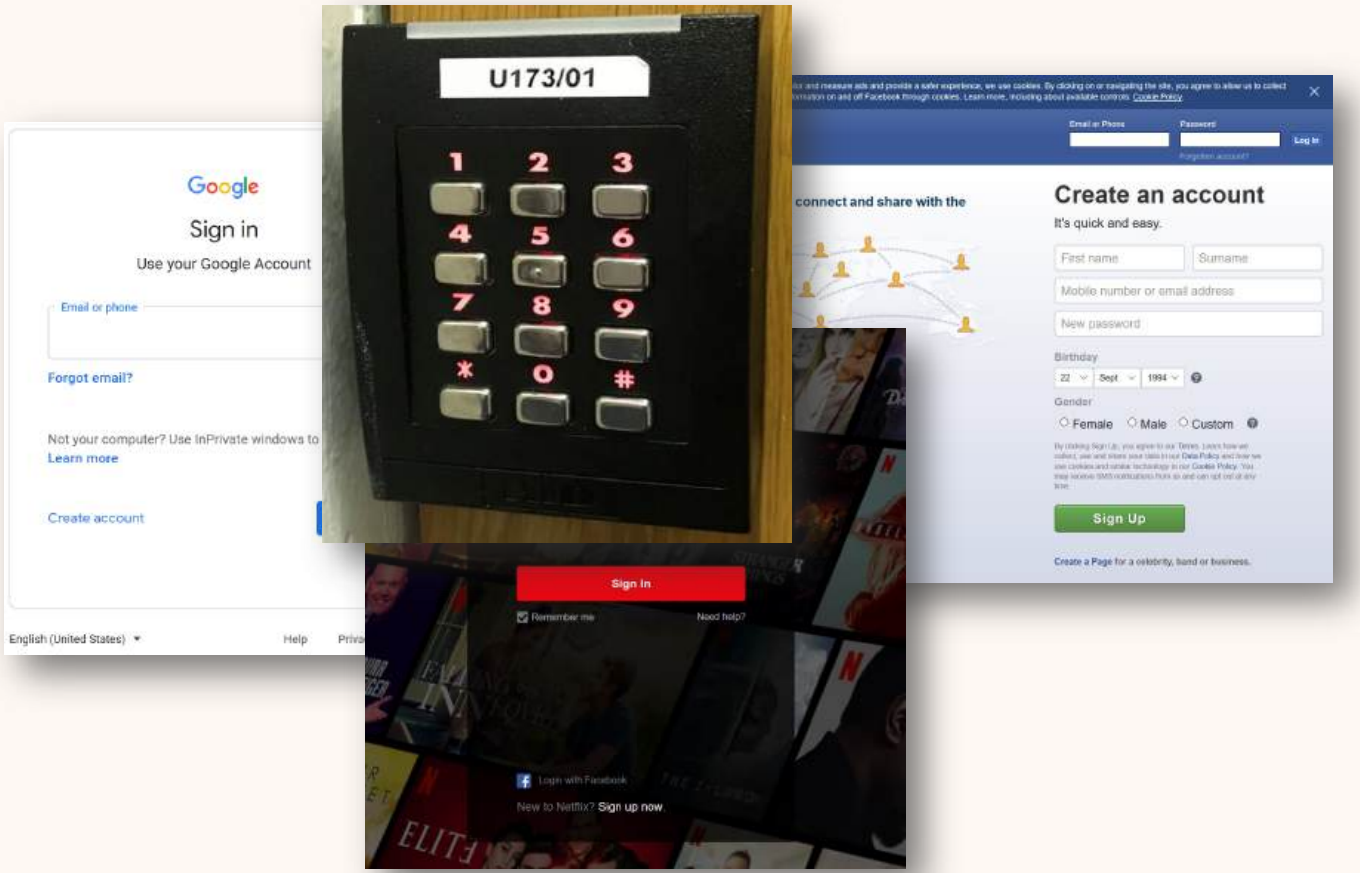
Security properties	
Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

Authentication vs. Authorization

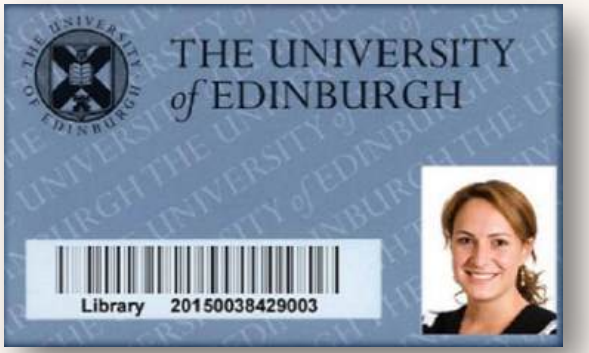
- Confidentiality: Ensures that computer-related assets are accessed only by **authorized** parties.

- Authentication – Process of **ensuring** that a person or device is **who they claim to be**.
- Authorization – Rules that **specify who is allowed to do what**.

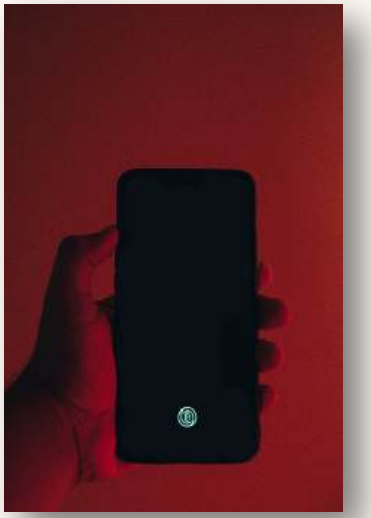
Authentication



What you know



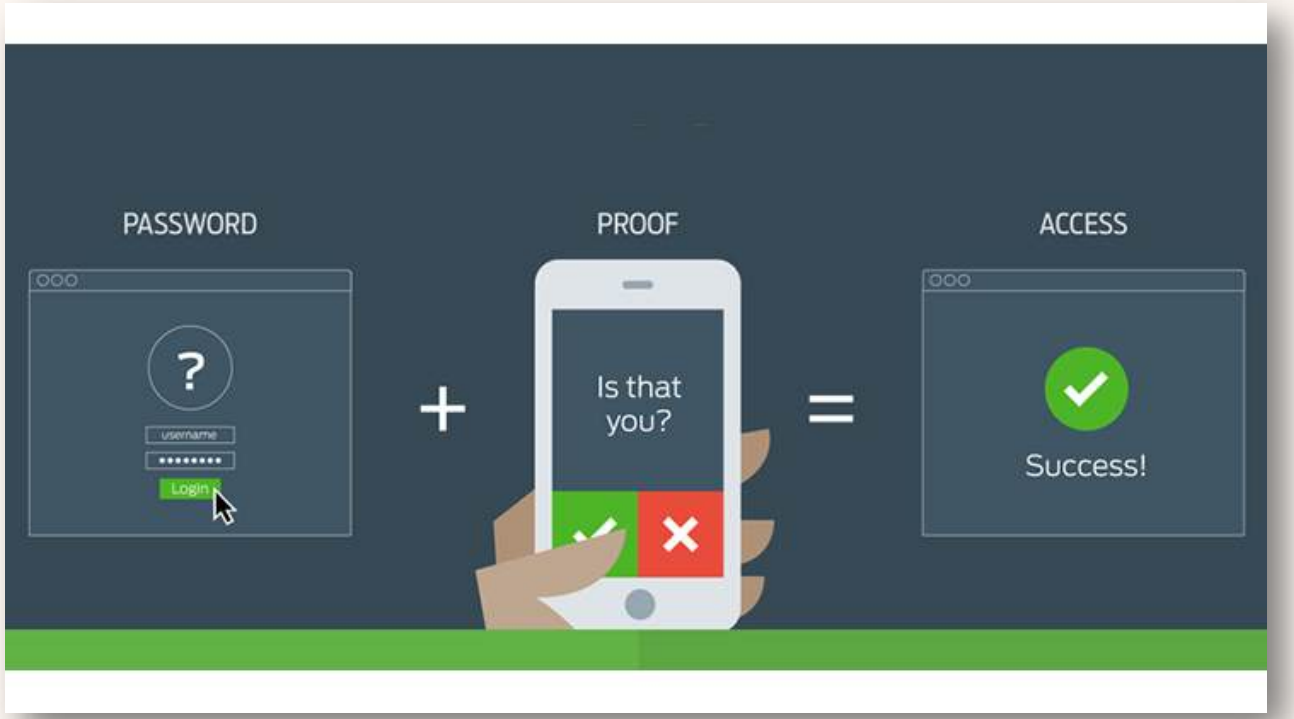
What you have



Who you are

Multi-factor authentication

- Requiring two or more separate and distinct forms of authentication methods



https://news.mit.edu/2015/two-factor-authentication-duo-security-0130

Usable Authentication is:

- User friendly
- Reasonable to implement
- Protects against attacks

Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

Is your university ID card “usable”?

Easy to use?

Easy for the university to implement?

Protects against attacks?
- Who wants to attack it?

Getting your first card

Information on getting your first University card and guidelines on submitting a photo.

University card functions

Your University card provides identification, library membership, printing, cashless catering and building access.

Replacement cards

If your University card or Library card has expired or is lost, stolen or damaged it can be replaced by a Card Help Desk.

Card Help Desks

Replacement cards can be requested at any of the University Library Card Help Desks.

Many ways exist to authenticate a person over just the web.

Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonatio*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Veri*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]	○	●	○	○	●	●	●	○	●	●	●	○	●	●	○	○					●	●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	○	●	○	●	○	●	●	○	○					●	●	○	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	○	●	●	○	○	○	○	○	○	●	●	○	●	●
Proxy	URRSA	IV-B	[5]	●	○	○	●	●	○	●	○	○	●	○	●	●	○	○	○			○		●	●	○	●	●
	Impostor		[23]	○	●	●	●	●	○	○	●	●	○	●	○	○	●	●	○			○		●	●	○	●	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	○	●	●	●	○	○	○	○		●		●	○	●	○
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	○	○	●	●	○	○	○	○	○		●		●	○	●	○
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	○	○	●	●	○	○	○	○	○		●		●	○	●	○
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	○	○	●	○	○	○	○	○		●		●	○	●	○
	OTP over email		[46]	○	●	●		●	○	○	●	●	●	○	●	●	○	○	○	○	○		●	●	●	○	●	○
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	○	●	○	●	○	●		●	○				●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	○	●	○	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	○	●	○	●	○	○		●						●	●	●	●
	Weinshall		[48]			●		○	○	○	○	○	●	○	●	○	●		●					●	●	●	●	●
	Hopper Blum		[49]			●		○	○	○	○	●	●	○	●	○	●	○	●					●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	○	●	○	●		○							●	●	●
Paper tokens	OTPW	IV-F	[33]			○		●	○	○	●	○	●	○	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		○		●	○	○	●	○	●	○	●	●	●		●	●	●	●	●	○	●	●	●	●
	PIN+TAN		[51]			○		●	○	○	○	○	○	○	●	●	●		●	●	●	●	●	●	●	●	●	●
Visual crypto	PassWindow		[52]	●		○		○	○	○	○	○	○	○	●	●	●	○	●	●	●	●	○	●	●	○	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			○		●	○	○	○	○	○	○	●	●	○		●	●	●	●	●	●	●	○	●	●
	YubiKey		[53]			○		●	○	○	○	●	○	○	●	●	○		●	●	●	●	●	●	●	○	●	●
	IronKey		[54]	○	●	○	○	○	○	○	○	●	○	●	●	●	○		●	○		○		●	●	●	●	●
	CAP reader		[55]			○		●	○	○	○	○	○	○	●	●	○		●	●	●	●	●	●	●	●	●	●
	Pico		[8]	●	●	○	●	○	○	○	○	○	○	○	○	●	○		●	●	●	●	●	●	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	○	○	○	○	○	○	○		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	○	○	○	○	●	●	○		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	○	○	○	○	○	○	○	●		○						●	●	●	●
	OTP over SMS			●	●	○		●	○	○	○	○	○	○	○	●	●		●	●	●	○	●	●	●	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	○	○	●	●	○		○	○	○	●		●	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●	●	●	○	●	○			○				○			●	●						●	●	
	Iris		[39]	●	●	●	○	●	○			○				○			●		●					●	○	
	Voice		[40]	●	●	●	○	●	○			○	○		○	○			●		○					●	●	
Recovery	Personal knowledge		[58]	○		●		●	○	●	○	●	●		●	●				●						●	●	
	Preference-based		[59]	○		●		●	○	○	○	●	●		●	●				○					●	●	●	
	Social re-auth.		[60]			●		●		●		●	●		●	○		○			●	●	○	●	●		●	○

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
= better than passwords; = worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

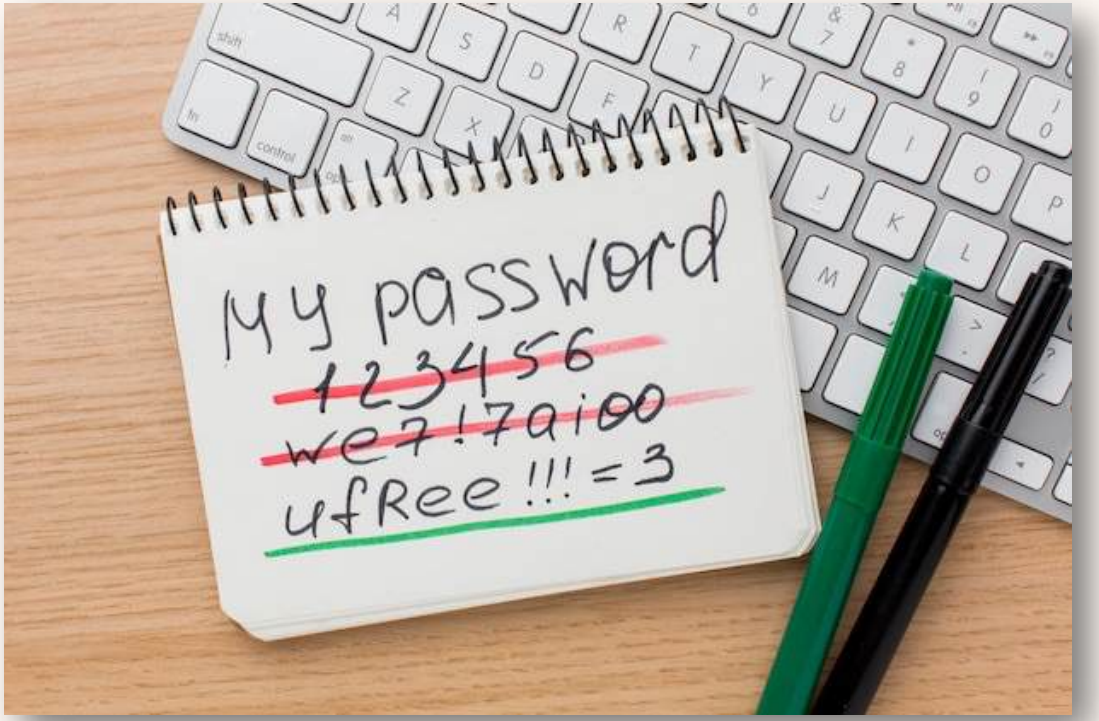
Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Passwords
Text **string** that is **theoretically only known by the end user**. The user authenticates by providing the string to the **server which then verifies** that it is the correct one.



Passwords
Text string that is theoretically only known by the end user. The user authenticates by providing the string to the server which then verifies that it is the correct one.

Wikipedia, List of the most common passwords
https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

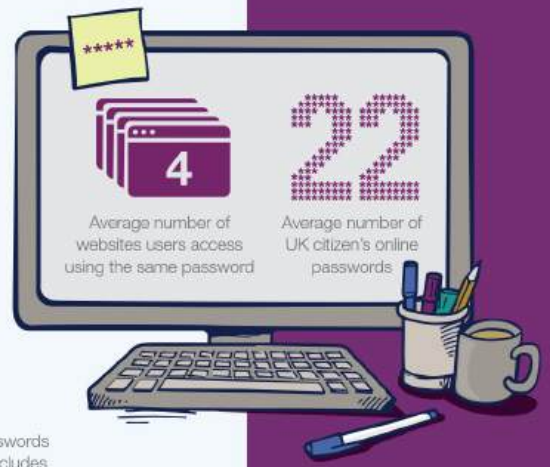
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc

What do people think a “good” password looks like?

Do Users' Perceptions of Password Security Match Reality?

Blase Ur, Jonathan Bees[†], Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University, [†]The Pennsylvania State University
{bur, ssegreti, lbauer, nicolasc, lorrie}@cmu.edu, [†]jfb5406@psu.edu

ABSTRACT
Although many users create predictable passwords, the extent to which users realize these passwords are predictable is not well understood. We investigate the relationship between users' perceptions of the strength of specific passwords and their actual strength. In this 165-participant online study, we ask participants to rate the comparative security of carefully juxtaposed pairs of passwords, as well as the security and memorability of both existing passwords and common password-creation strategies. Participants had serious misconceptions about the impact of basing passwords on common phrases and including digits and keyboard patterns in passwords. However, in most other cases, participants' perceptions of what characteristics make a password secure were consistent with the performance of current password-cracking tools. We find large variance in participants' understanding of how passwords may be attacked, potentially explaining why users nonetheless make predictable passwords. We conclude with design directions for helping users make better passwords.

chosen to exhibit particular characteristics, as well as common strategies for password creation and management. We compare participants' perceptions to the passwords' actual resilience to a variety of large-scale password-guessing attacks.

In the first of four tasks, we showed participants 25 pairs of passwords differing in specific characteristics (e.g., appending a digit, as opposed to a letter, to the end of the password). We asked participants to rate which password was more secure, if any, and to justify their rating in free text. In the second and third tasks, we showed participants a selection of passwords from the well-studied breach of the website RockYou [72], as well as descriptions of common password-creation strategies. We asked participants to rate both the security and the memorability of each password or strategy. In the fourth task, we had participants articulate their model of password attackers and their expectations for how attackers try to guess passwords.

We observed some serious misconceptions about password security. Many participants overestimated the benefits of including digits, as opposed to other characters, in a password. Many

Which one is stronger, “questionnaires” or “iloveliverpool”?

Misconception of password security

- Adding digits to letters is better than letters only (not really, as adversaries already exploited this tendency)
- Keyboard patterns are more secure? Wrong.
- Changing certain characters, e.g. o->0, may not always work!
- People misjudging the popularity of certain words and phrases – “questionnaires” is more secure than “iloveliverpool”

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N. and Cranor, L.F., 2016, May. Do users' perceptions of password security match reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3748-3760).

NCSC Good password practices

- Avoid the common passwords and using your personal info
- Long and strong (e.g., some combination of three random words)
- Using password managers
- Changing certain characters, e.g. o->0, may not always work!

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words#:~:text=A%20good%20way%20to%20make,(like%20'password').

A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Good Poor Bad

Passwords

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

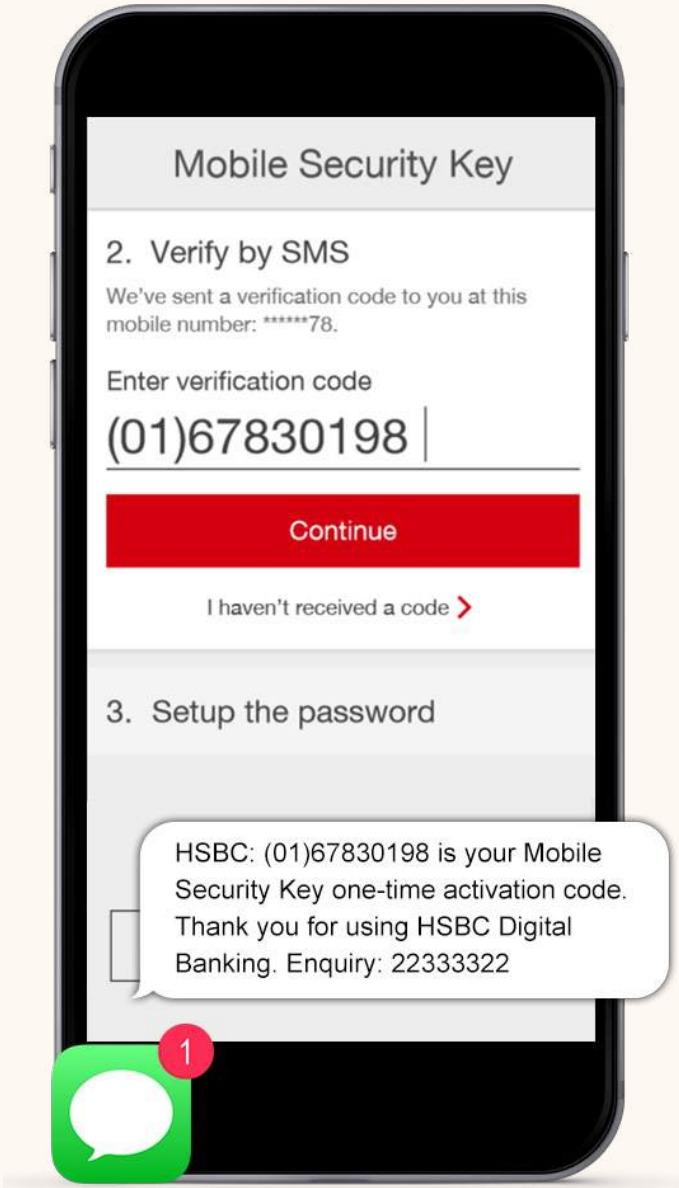
Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Are SMS-based one time passwords more or less usable than normal passwords?



One time password over SMS

Good Poor Bad

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

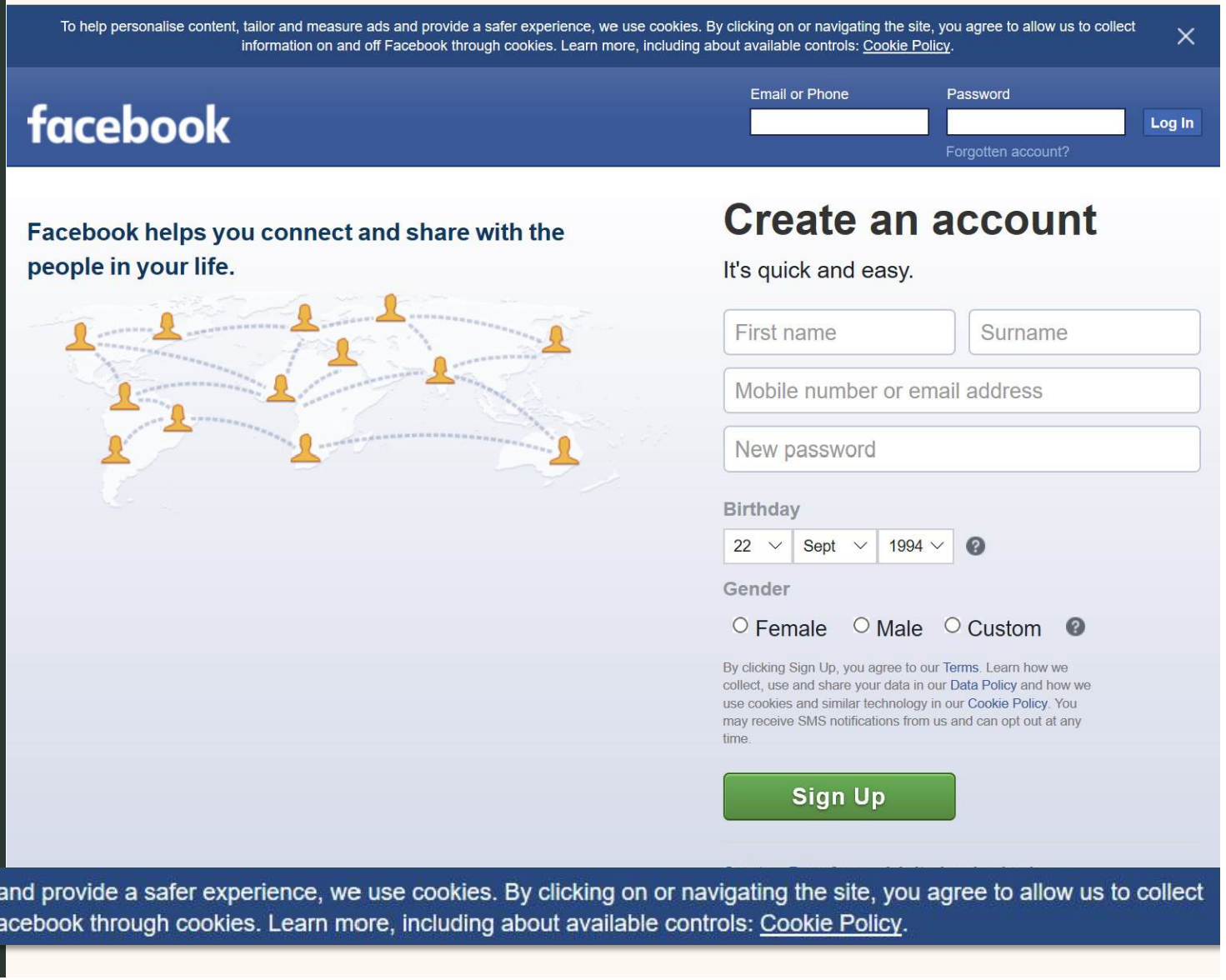
Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Passwords
Text string that is theoretically only known by the end user. The user authenticates by providing the string to the server which then verifies that it is the correct one.



A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Good Poor Bad

Cookies + Passwords

User friendly

? Memory effortless

- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

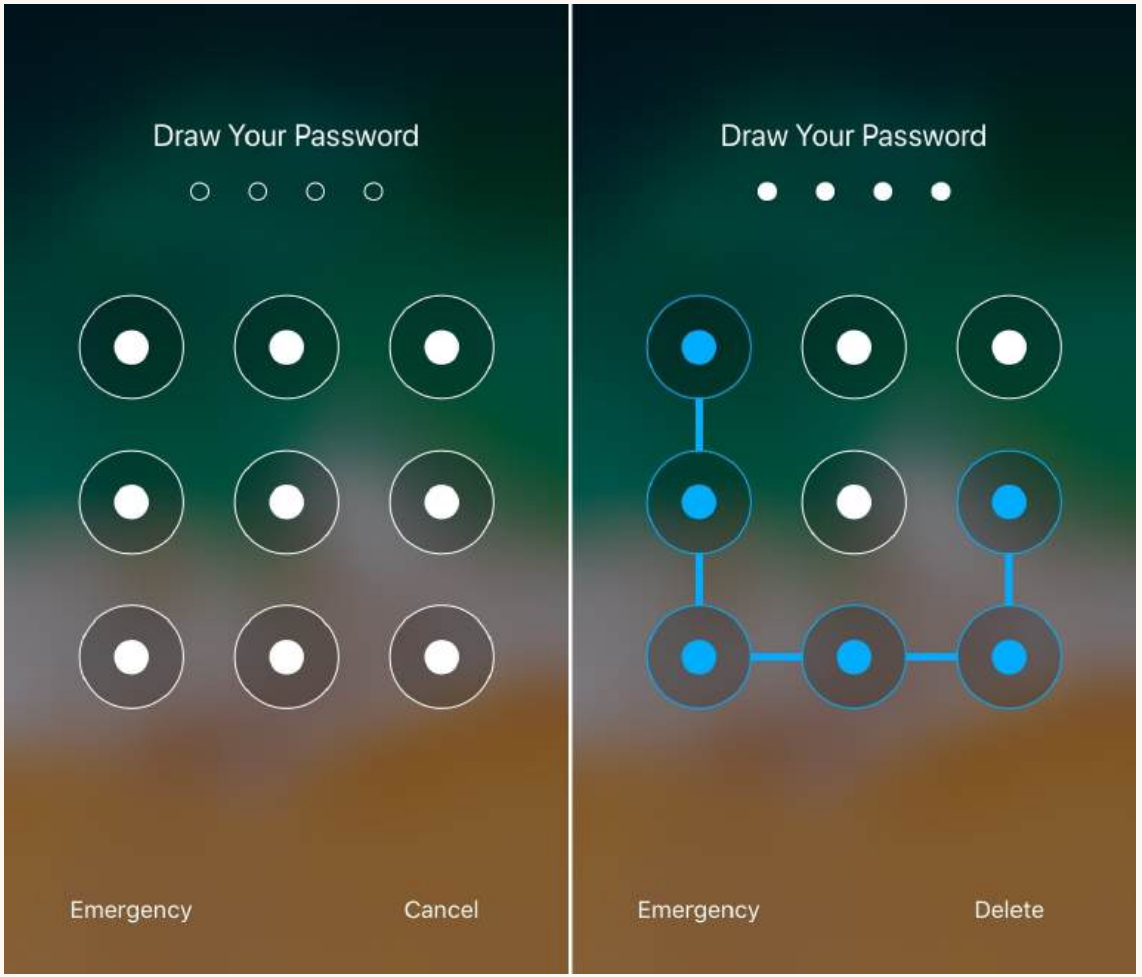
Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Passwords
Text string that is theoretically only known by the end user. The user authenticates by providing the string to the server which then verifies that it is the correct one.



A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Find it out!

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

How to nudge people to pick stronger passwords?

How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass,
Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{*bur, pgage, sarangak, jlee, mmaass, mmazurek, tpassaro,*
rshay, tvidas, lbauer, nicolasc, lorrie}*@cmu.edu*

Abstract

To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied.

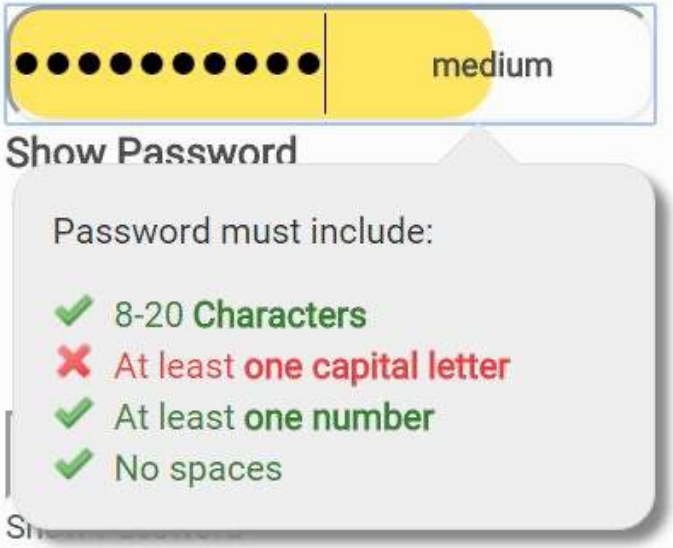
We present a 2,931-subject study of password creation in the presence of 14 password meters. We found that meters with a variety of visual appearances led users to create longer passwords. However, significant increases in resistance to a password-cracking algorithm were only achieved using meters that scored passwords stringently.

or write them down [28]. Password-composition policies, sets of requirements that every password on a system must meet, can also make passwords more difficult to guess [6, 38]. However, strict policies can lead to user frustration [29], and users may fulfill requirements in ways that are simple and predictable [6].

Another measure for encouraging users to create stronger passwords is the use of password meters. A password meter is a visual representation of password strength, often presented as a colored bar on screen. Password meters employ suggestions to assist users in creating stronger passwords. Many popular websites, from Google to Twitter, employ password meters.

The effect of strength meters on password creation

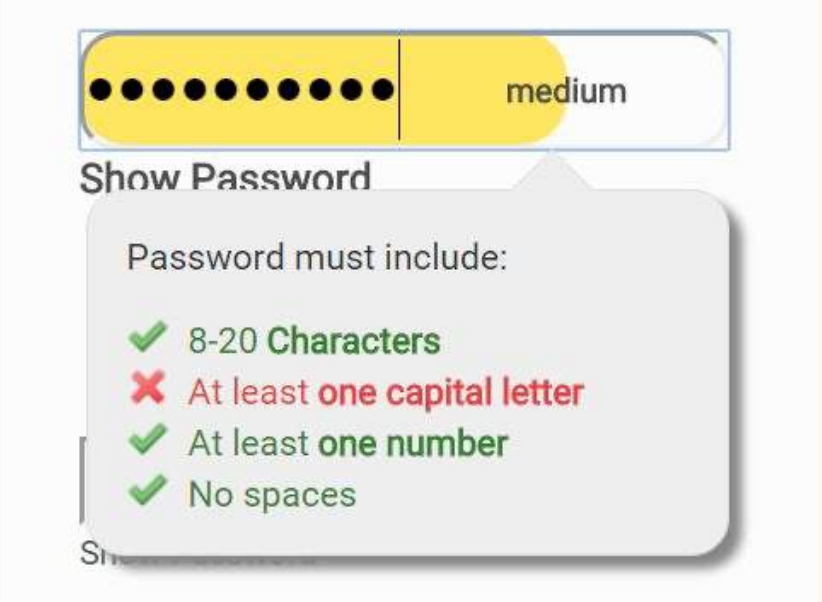
- Phase 1: What kinds of meters are being used by websites right now?
- Phase 2: What are “good” measures of password quality?
- Phase 3: How do different meter designs impact the passwords created? If so, which meters perform best?



Ur, Blase, et al. "How does your password measure up? The effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Phase 1: What kinds of meters are being used by websites right now?

- Reviewed login pages of Alexa top 100 most popular websites
- 96 allowed a login
- 70 gave some type of password feedback
- Common types of meters
  - Bar-like (50%)
  - Checkmark or X system (41.3\%)
  - Text indicating problems (21.2\%)



Ur, Blase, et al. "How does your password measure up? the effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Phase 1: Understand the security technology

- Good idea to start any security project by first **understanding the technology** you are working with.
  - Security concepts can often be non-obvious in how they work or interact with other technology.
- Determine the current **state-of-the-art**.
  - How do other people solve this problem now?
  - Why are they doing it that way and has anyone decided what solution is “best”?
- Formulate **a question about the technology** based on what you find.

Just colored words

Facebook

New: •••••

Too short

Re-type new: •••••

Passwords match

Baidu

Password: **Confirm Password:**

••••••

The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully.
Password length of 6 to 14, the letters are case-sensitive. Password is too simple hazards

Green bars / Checkmark-x

Twitter

••••••••

✖ Password is too obvious.

••••••••••

✓ Password is okay.

••••••••••••••••••••

✓ Password is perfect!

Checklists

Apple

••••••••

Password strength: weak

Password must:

- Have at least one letter
- Have at least one capital letter
- Have at least one number
- Not contain more than 3 consecutive identical characters
- Not be the same as the account name
- Be at least 8 characters

Segmented bars

Weibo

* Create a ••••••••

弱 中 強

弱 中 強

弱 中 強

Mail.ru

Уровень сложности: слабый

Уровень сложности: сильный

Paypal

Fair

- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- ▪ Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Strong
Fair
Weak

Yahoo.jp and Yahoo

baseball1 パスワードの安全性 低 Strong

Aaaaaa1! パスワードの安全性 中 Very strong

Gradient bars

Wordpress.com

Bad

Live.com

Weak

Medium

Strong

Color changing bars

Mediafire

••••

Password Strength Too short

Password Strength Weak

Password Strength Fair

Password Strength Good

Password Strength Strong

Blogger

••••••••

Password strength: Weak

Google

Create a password

••••••••

Password strength: Weak

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?

Password strength: Strong

Password strength: Good

Password strength: Too short

Phase 2: What are “good” measures of password quality?

- Look at scientific literature to understand what other people have already learned.
- Two well known ways to measure password strength:
  - **Basic16** - password must have at least 16 characters.
  - **Comprehensive8** – password must have at least eight characters, including an uppercase letter, a lowercase letter, a digit, and a symbol. It must also not already be in a wordlist of common passwords.

- password
- P@ssw0rd
- iloveyou123
- monkey
- thisisasuperlongpasswordthatisawesome
- VV@yBetter123

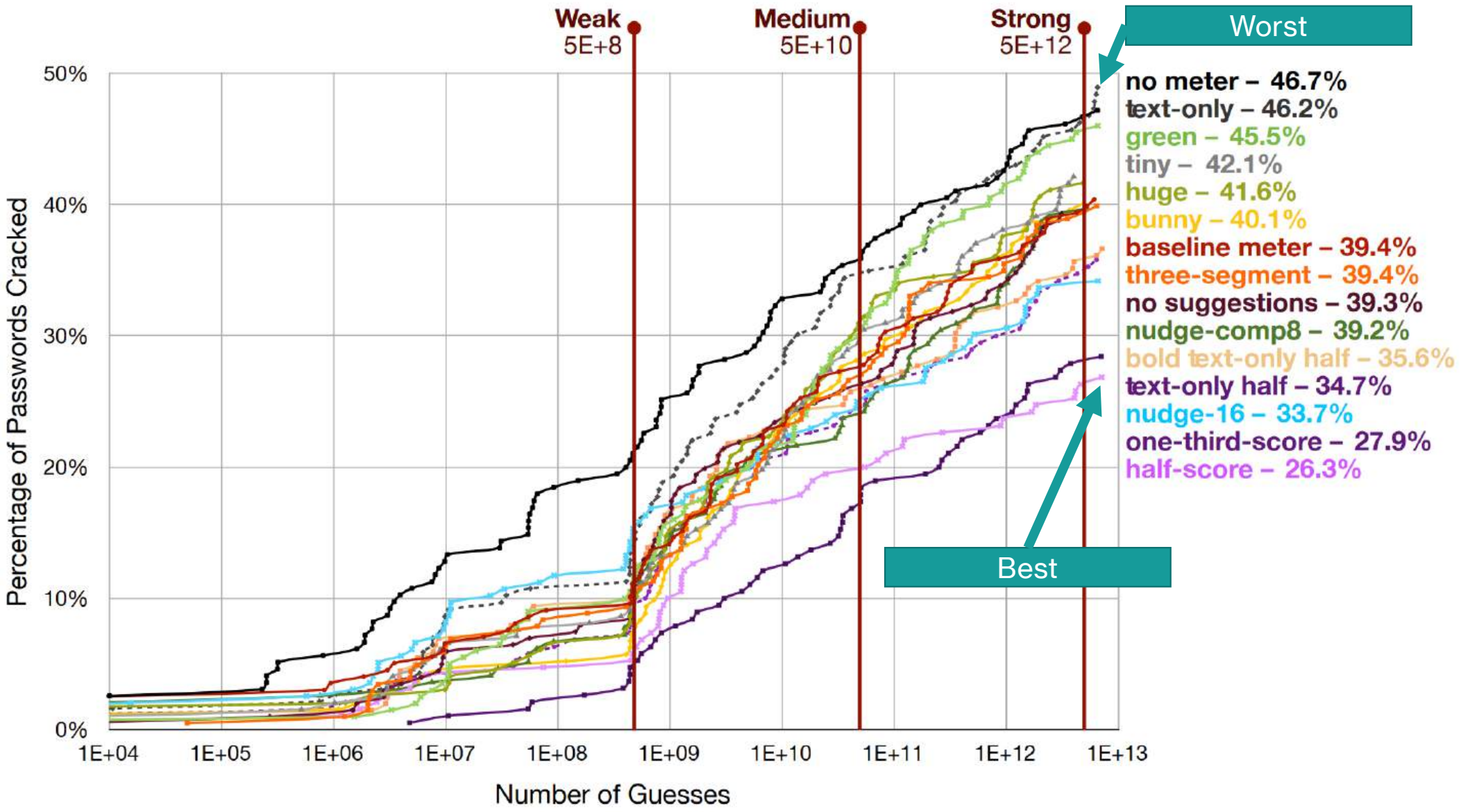
Phase 3: How do different meter designs impact the passwords created?

- Online survey study using Amazon Mechanical Turk
- 15 different conditions (next slide)
- 2931 participants
- 2 phase study:
  - Setup a password
  - 2 days later, log in using the original password

Ur, Blase, et al. "How does your password measure up? the effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Conditions

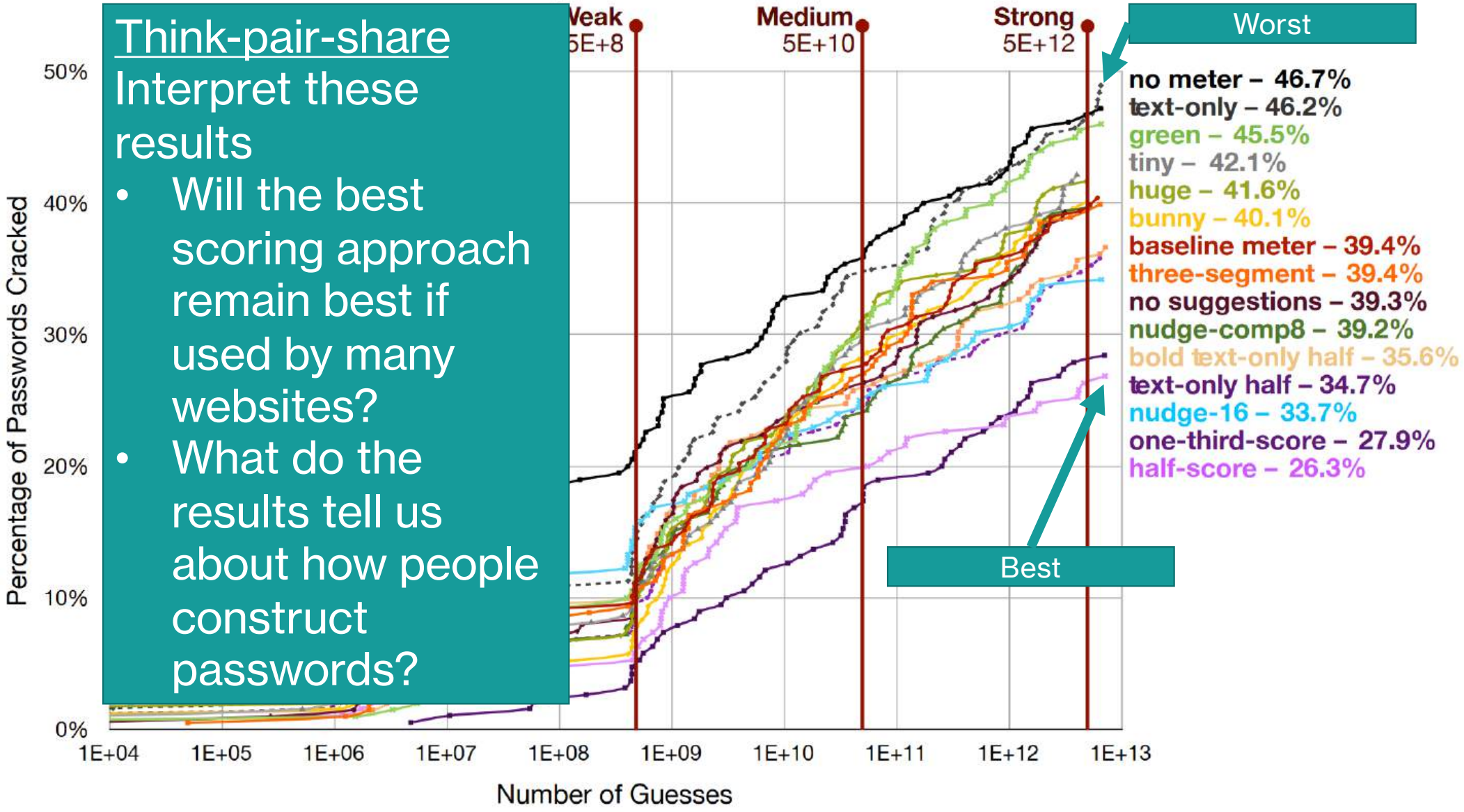
- **Control**
  - No meter
  - Baseline meter based on real ones – colored bar with text hints
- **Appearance variations**
  - Three-segment
  - Green – bar is always green
  - Tiny – bar is very small
  - Huge – bar is very large
  - No suggestions – bar, but no helpful feedback
  - Text-only – feedback, but no bar
- **Scoring**
  - Half-score – bar shown half as full as would be in baseline
  - One-third-score
  - Nudge-16 – score uses the Basic16 metric
  - Nudge-comp8 – score uses Comprehensive8 metric
- **Multiple variations**
  - Text-only & half-score
  - Bold text-only & half score
  - Bunny – running bunny instead of a meter


Weak
5E+8
Medium
5E+10
Strong
5E+12
Worst
Best
no meter – 46.7%
text-only – 46.2%
green – 45.5%
tiny – 42.1%
huge – 41.6%
bunny – 40.1%
baseline meter – 39.4%
three-segment – 39.4%
no suggestions – 39.3%
nudge-comp8 – 39.2%
bold text-only half – 35.6%
text-only half – 34.7%
nudge-16 – 33.7%
one-third-score – 27.9%
half-score – 26.3%
Percentage of Passwords Cracked
50%
40%
30%
20%
10%
0%
1E+04
1E+05
1E+06
1E+07
1E+08
1E+09
1E+10
1E+11
1E+12
1E+13
Number of Guesses

Think-pair-share

Interpret these results

- Will the best scoring approach remain best if used by many websites?
- What do the results tell us about how people construct passwords?



Takeaway

- Stringency helps, but to some extent
- Combination of text and visual indicator works better than only each of them
- People’s behavior changed through password creation with the meter

Questions?

Take-home

- **(blog)** Stephenson, S., Pal, B., Fan, S., Fernandes, E., Zhao, Y. and Chatterjee, R., 2022, May. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 267-284). IEEE.
- **(blog)** The register -- Fortinet: FortiGate config leaks are genuine but misleading