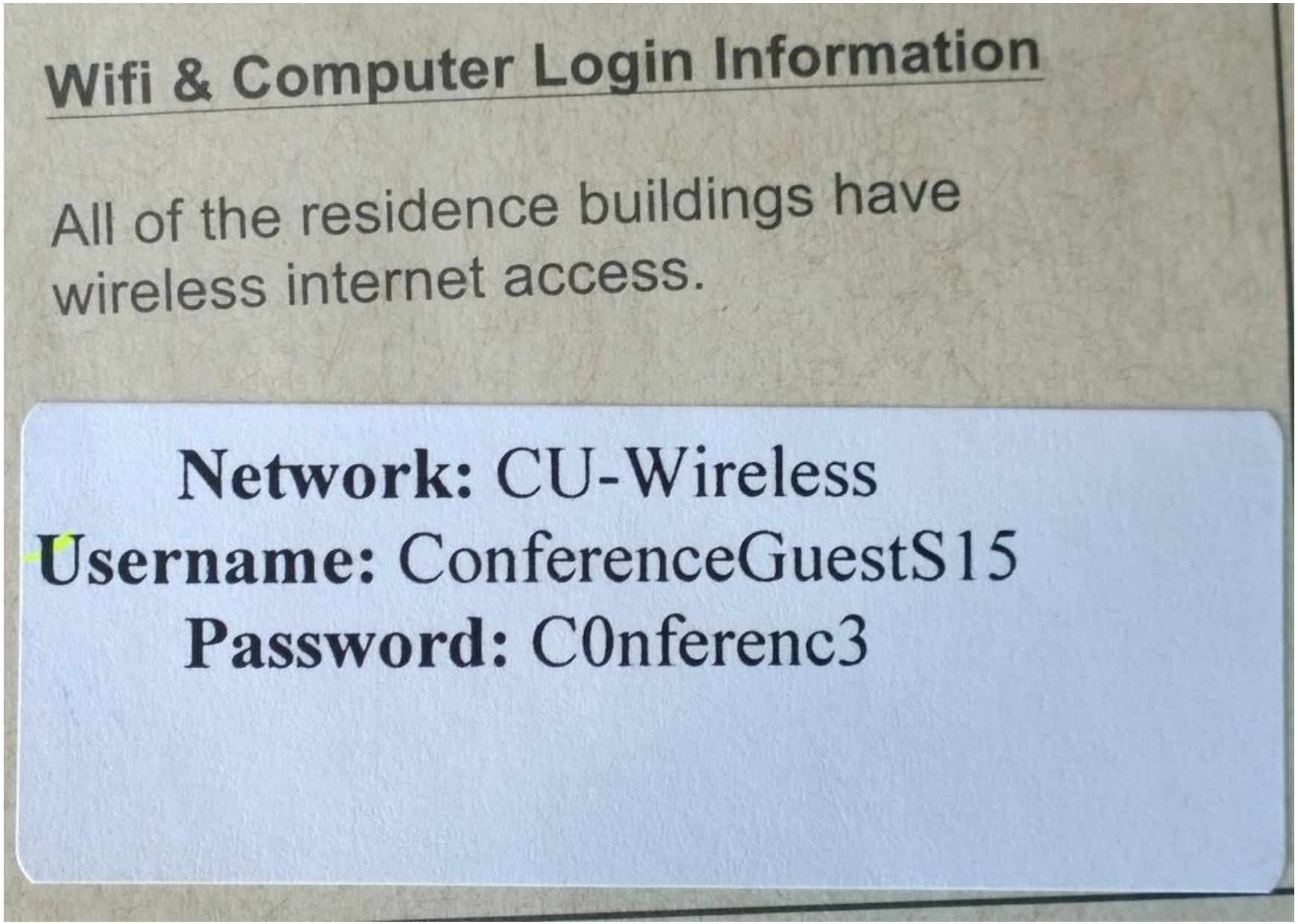
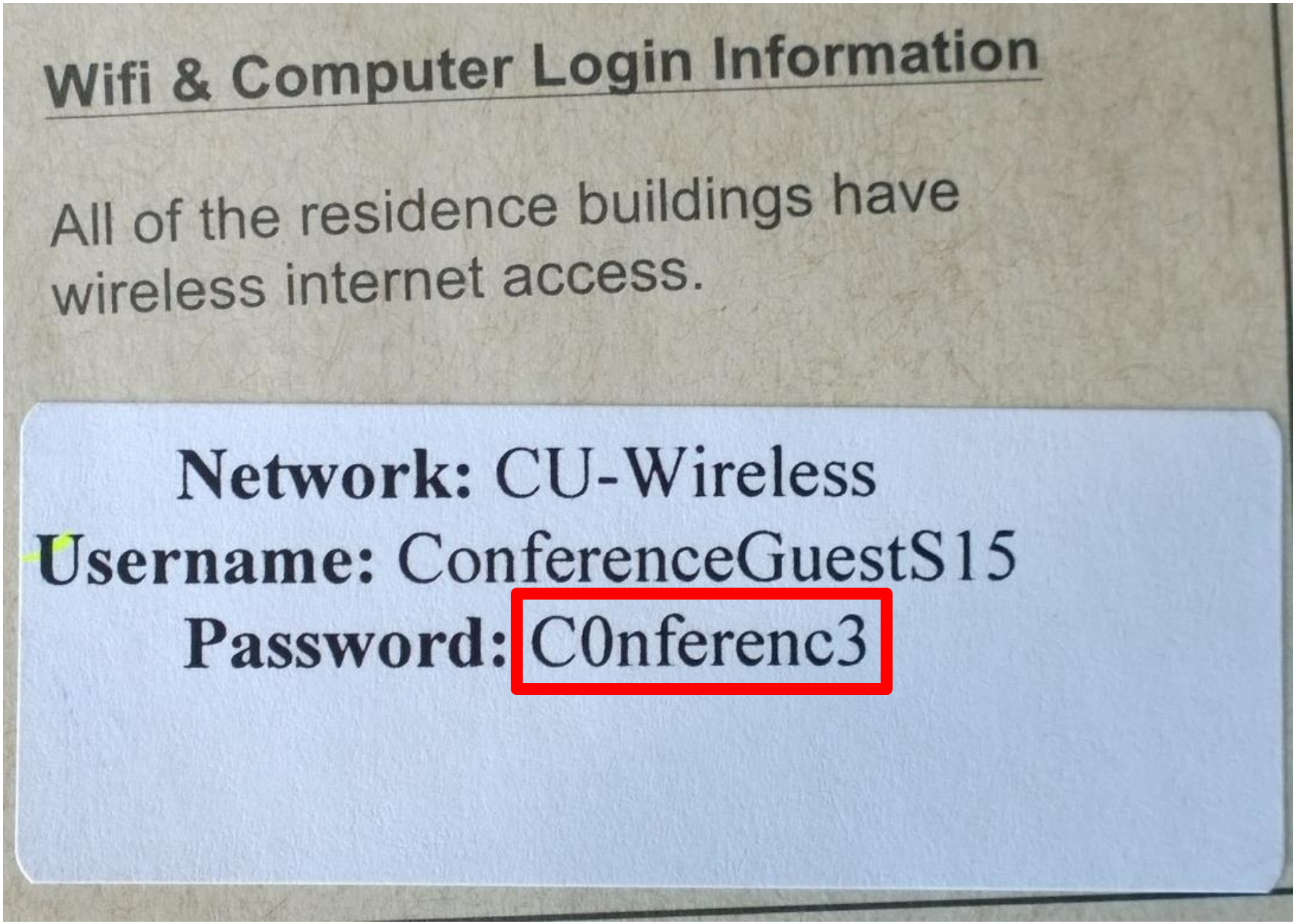
“I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab

Blase Ur, Fumiko Noma, Jonathan Bees,
Sean M. Segreti, Richard Shay, Lujo Bauer,
Nicolas Christin, Lorrie Faith Cranor

Carnegie Mellon

123456789
12345
password
iloveyou
princess
rockyou
1234567
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
football
secret
andrea
carlos
jennifer
jasmine
bubbles
basketball
superman
hottie
tinkerbell
elizabeth
brandon
playboy
pretty
666666
whatever
lovers
dragon
spongebob
cookie
flower
andrew
chelsea
angels
matthew
shadow
summer
melissa
barbie
hannah
samantha
eminem
1234567890
softball
hello
computer
robert
jesus
mickey
poohbear
danielle


Wifi & Computer Login Information
All of the residence buildings have wireless internet access.
Network: CU-Wireless
Username: ConferenceGuestS15
Password: C0nferenc3


Wifi & Computer Login Information
All of the residence buildings have wireless internet access.
Network: CU-Wireless
Username: ConferenceGuestS15
Password: C0nferenc3

SSH Username: root Password: HTPassw0rd

SSH Username: root Password: HTPassw0rd

12345
password
123456789
iloveyou
princess
rockyou
1234567
12345678
babygirl
654321
jessica
monkey
angel
soccer
flower
carlos
eminem
nicole
liverpool
tigger
michael
purple
shadow
andrea
tinkerbell
password1
ashley
daniel
anthony
lovely
jordan
football
playboy
666666
jasmine
chelsea
pretty
secret
angels
justin
andrew
qwerty
abc123
butterfly
superman
basketball
brandon
elizabeth
chocolate
jennifer
robert
bubbles
dragon
hottie
cookie
michelle
softball
matthew
sunshine
charlie
spongebob
forever
whatever
christian

password

ilovebillyC$1

ilovebillyC$1

ilovebillyC$1

AfNaHiLoco

AfNaHiLoco

Goals

- Understand precisely how people make passwords
  - In-lab, think-aloud protocol

Goals

- Understand precisely how people make passwords
  - In-lab, think-aloud protocol
- How users assign value to accounts

Goals

- Understand precisely how people make passwords
  - In-lab, think-aloud protocol
- How users assign value to accounts
- Users' password-creation processes

Goals

- Understand precisely how people make passwords
  - In-lab, think-aloud protocol
- How users assign value to accounts
- Users' password-creation processes
- "Microdecisions" users think add security

Methodology

- 49-participant lab study

Methodology

- 49-participant lab study
- Recruited using flyers / Craigslist

Methodology

- 49-participant lab study
- Recruited using flyers / Craigslist
- 45 – 60 minutes, compensated $25

Methodology

- Think aloud while creating 3 passwords:

Methodology

- Think aloud while creating 3 passwords:

Methodology

- Think aloud while creating 3 passwords:

Methodology

- Think aloud while creating 3 passwords:

Methodology

- Follow-up questions to understand why

Methodology

- Follow-up questions to understand why
- Questions about general strategies

Methodology

- Follow-up questions to understand why
- Questions about general strategies
- Following distraction task, recall password

Security Metric: Guessability

- Guessability – how many guesses to crack?
  - Threat model: large-scale guessing

Security Metric: Guessability

- Guessability – how many guesses to crack?
  - Threat model: large-scale guessing

- 10^{14} guesses using Hashcat

Security Metric: Guessability

- Guessability – how many guesses to crack?
  - Threat model: large-scale guessing
- 10^{14} guesses using Hashcat
- User-specific and site-specific attacks

Qualitative Analysis

- Based on affinity diagramming

Qualitative Analysis

- Based on affinity diagramming
  - Collaboratively grouped 546 behaviors / strategies

Qualitative Analysis

- Based on affinity diagramming
  - Collaboratively grouped 546 behaviors / strategies

- 25 broad themes
  - 122 distinct behaviors

Limitations

- Small-scale, non-representative sample
- Limited ecological validity
  - Only one use of passwords
  - Test recall in same session

Results Outline

- Overview of participants
- Overview of passwords
- Security levels
- Strategies

Participants

- 49 participants
  - 21 male
  - 28 female

Participants

- 49 participants
  - 21 male
  - 28 female

- Variety of occupations
  - 24 students
  - 16 employed
  - 9 unemployed/retired

Participants

- 49 participants
  - 21 male
  - 28 female
- Variety of occupations
  - 24 students
  - 16 employed
  - 9 unemployed/retired
- Mean age 31 (median 24)

Passwords

Passwords

- Transformed (Fahl et al., SOUPS 2013)

Passwords

- Transformed (Fahl et al., SOUPS 2013)
- 6 passwords trivially guessable
  - *gabriel*, *Password1!*

Passwords

- Transformed (Fahl et al., SOUPS 2013)
- 6 passwords trivially guessable
  - *gabriel*, *Password1!*
- Half of passwords guessed
  - e.g., *Tyrone1975*, *Gandalf*8*, *Triptrip1963*

Passwords

- Transformed (Fahl et al., SOUPS 2013)
- 6 passwords trivially guessable
  - *gabriel*, *Password1!*
- Half of passwords guessed
  - e.g., *Tyrone1975*, *Gandalf*8*, *Triptrip1963*
- Half of passwords secure
  - e.g., *5cupsoftoys*, *AfNaHiLoco*, *7301Poplarblvd$*

Security Levels

Security Levels

- 21 participants considered sites equal value

Security Levels

- 21 participants considered sites equal value
- Struggled matching password to security level

Security Levels

- 21 participants considered sites equal value
- Struggled matching password to security level
  - P6's high-value passwords both guessed

Security Levels

- 21 participants considered sites equal value
- Struggled matching password to security level
  - P6's high-value passwords both guessed
- Creating a password "stresses me out…I know I want a really strong password. Thinking through how I want to create that is tough." (P18)

Strategies

Base password on site

Base password on site

- Insecure banking password

```
+Money369
```

Base password on site

- Insecure banking password

+Money369

Base password on site

- Insecure banking password

+Money369

Base password on site

- Secure news password

```
LEFTbrown8!
```

Base password on site

- Secure news password

LEFTbrown8!

Please create a new password for your news account.

Base password on site

- Secure news password

LEFTbrown8!

Base password on site

- Secure news password

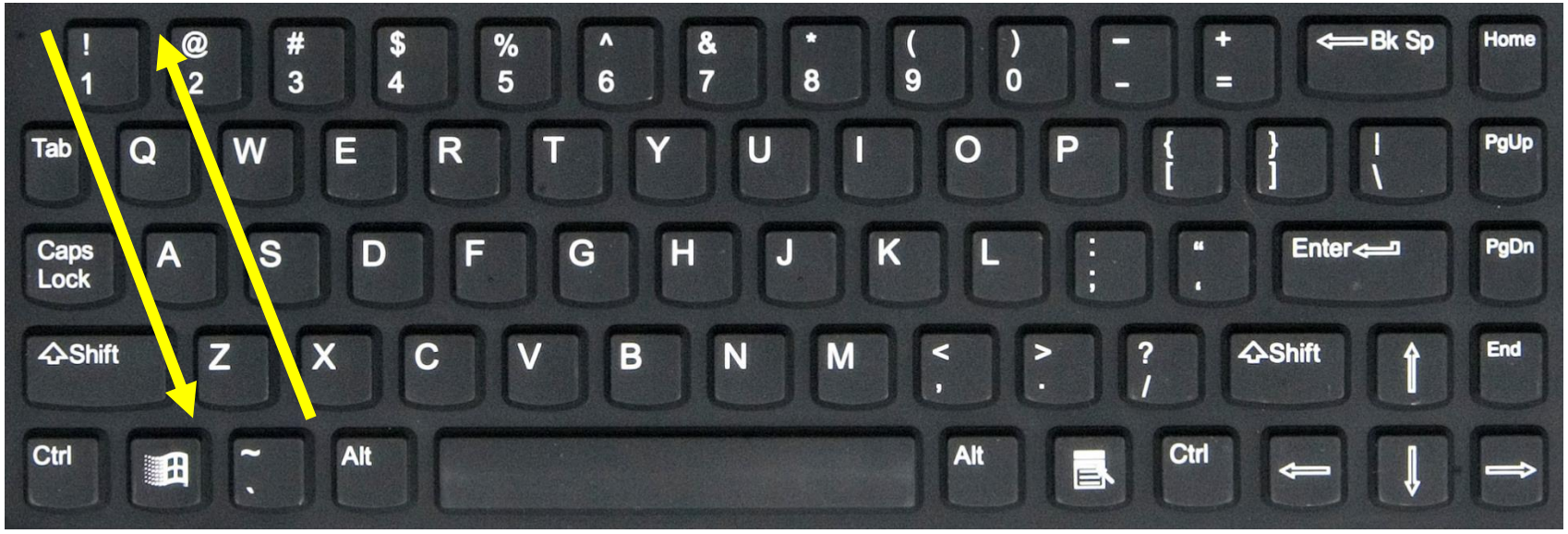
LEFTbrown8!

Knew to avoid dictionary words

Knew to avoid dictionary words

- Insecure keyboard patterns

```
1Qazxsw2
```



Knew to avoid dictionary words

- Secure (believed insecure)

`junglesalmon711`

Knew to avoid dictionary words

- Secure (and believed secure)

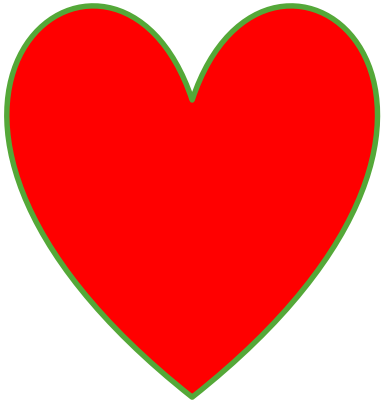
`Rjunglesalmon711@$`

Build password around phrase

Build password around phrase

- Insecure

```
ilove1sttrust!
```



First Trust
National Bank

Please create a new password for your banking account.

Build password around phrase

- Secure

```
AfNaHiLoco
```

Build password around phrase

- Secure

`AfNaHiLoco`

Afraid of the Native Hipsters
Loopily Coding

Build password around phrase

- *Be the change* because “someone wouldn’t think it necessarily applies to me” (P17)

Digits and symbols make it secure

- Insecure

Tyrone

Digits and symbols make it secure

- Insecure (believed secure)
  - “Security is required for a bank account” (P37)

```
Tyrone1975
```

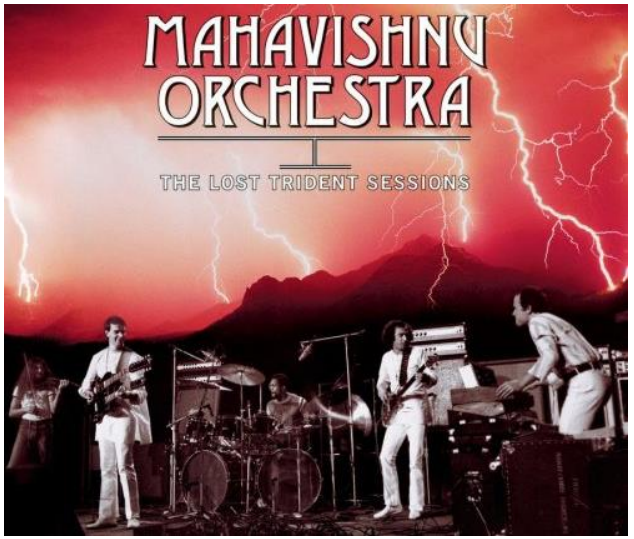
Digits and symbols make it secure

- “I added ‘!’ at the end to make it secure.” (P45)

Misunderstanding attackers

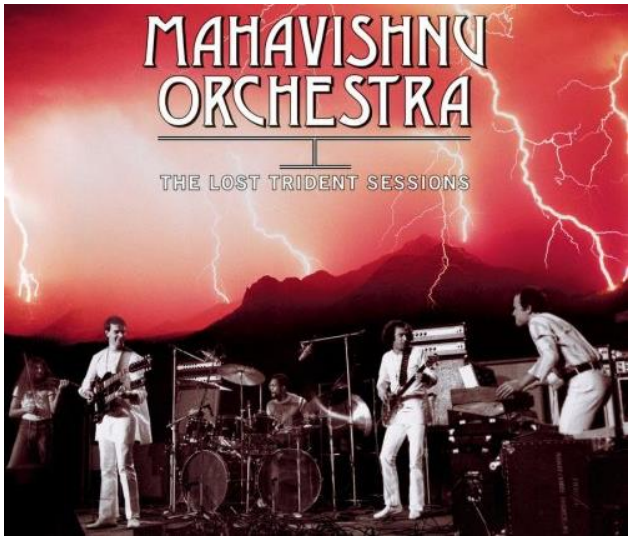
Misunderstanding attackers

- Mahavishnu Orchestra is secure because “this band name is hard to spell” (P2)



Misunderstanding attackers

- Mahavishnu Orchestra is secure because “this band name is hard to spell” (P2)



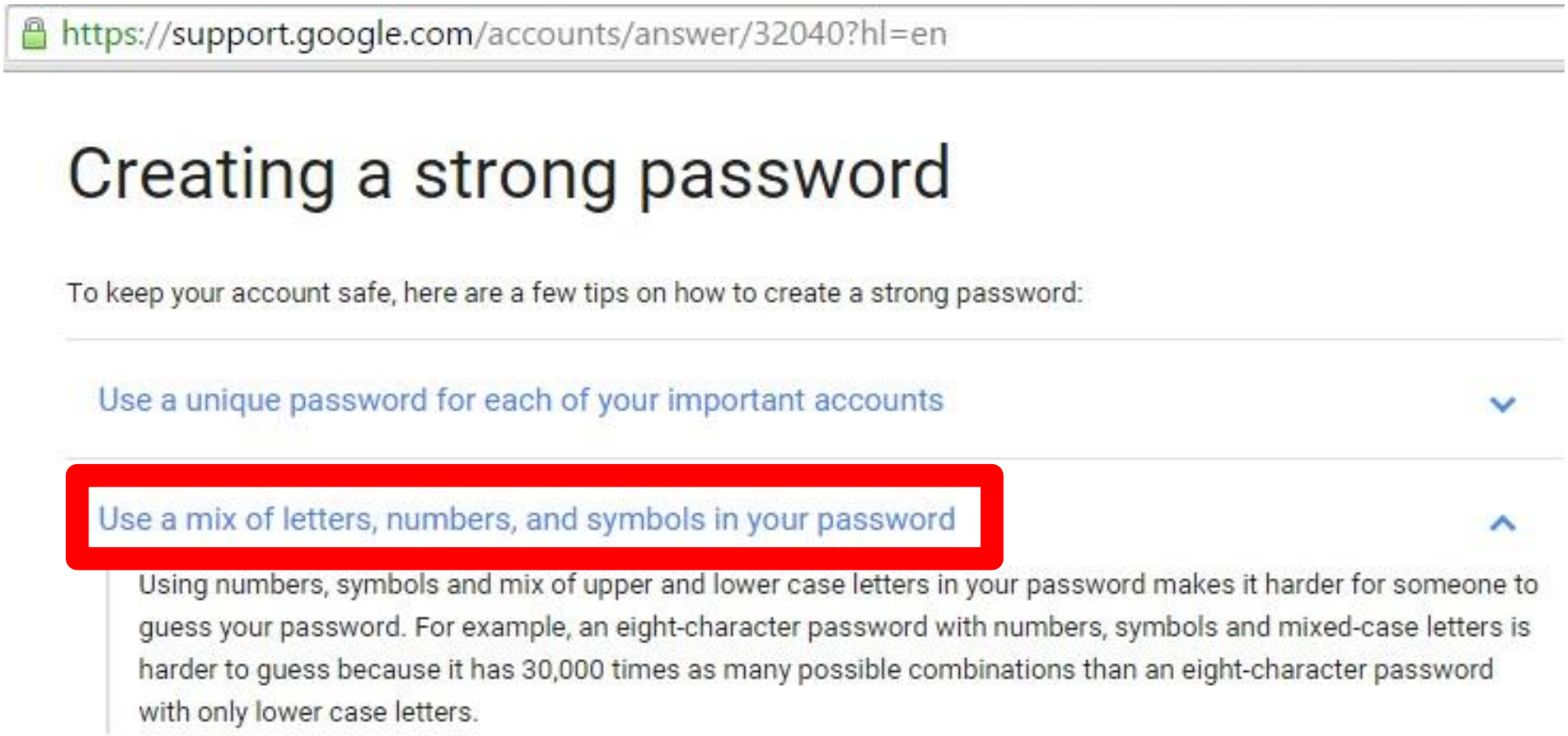
- Goldie: “hackers cannot guess [it] because I have no pictures of him on my Facebook account.” (P7)

Conclusions

- Users had process, yet many misconceptions

Conclusions

- Users had process, yet many misconceptions



Conclusions

- Users had process, yet many misconceptions

Cannot Contain:

- known personal information
- last five passwords
- four or more occurrences of same character*
- a Dictionary word* (after removing non-alpha characters)

Conclusions

- Users had process, yet many misconceptions

Cannot Contain:

- known personal information
- last five passwords
- four or more occurrences of same character*
- a Dictionary word* (after removing non-alpha characters)

Future Directions

Future Directions

- Help users assign value to accounts

Future Directions

- Help users assign value to accounts
- Promote secure creation processes

Future Directions

- Help users assign value to accounts
- Promote secure creation processes
- Data-driven tools

“I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab

Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

Carnegie Mellon

Password Guessability Service