RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M01

Opening Remarks: Security, Privacy & Human Behavior

Lorrie Cranor

Director, CyLab Security and Privacy Institute
Carnegie Mellon University
@lorrietweet

the INQUIRER

industryvoice

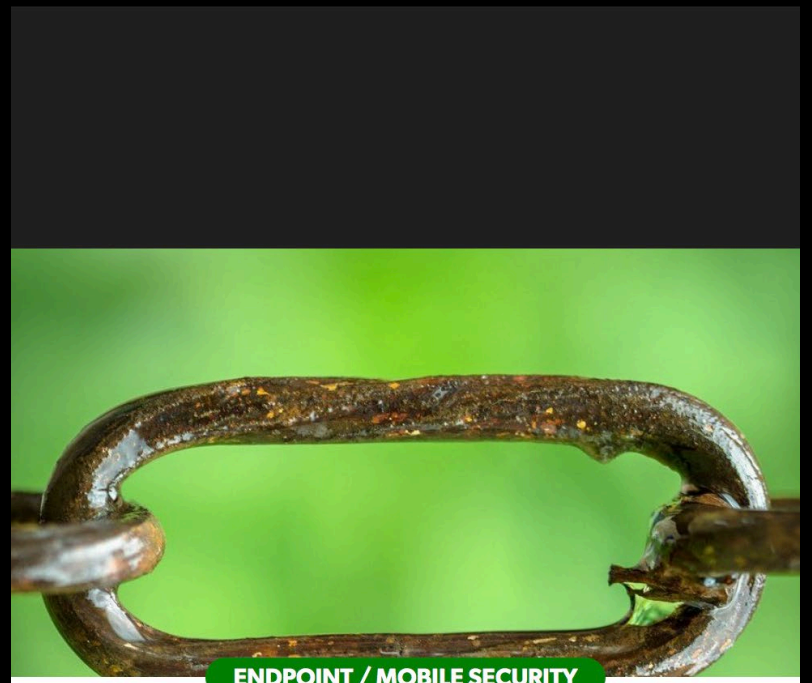
Security

Human error is the root cause of most data breaches

Financial damage of data leaks must be considered by firms

Markel Direct

SECUREWORLD
See globally. Defend locally.



ENDPOINT / MOBILE SECURITY

The Weakest Link: The Role of Human Error in Cybersecurity

Chief Executive

CEOs in the News

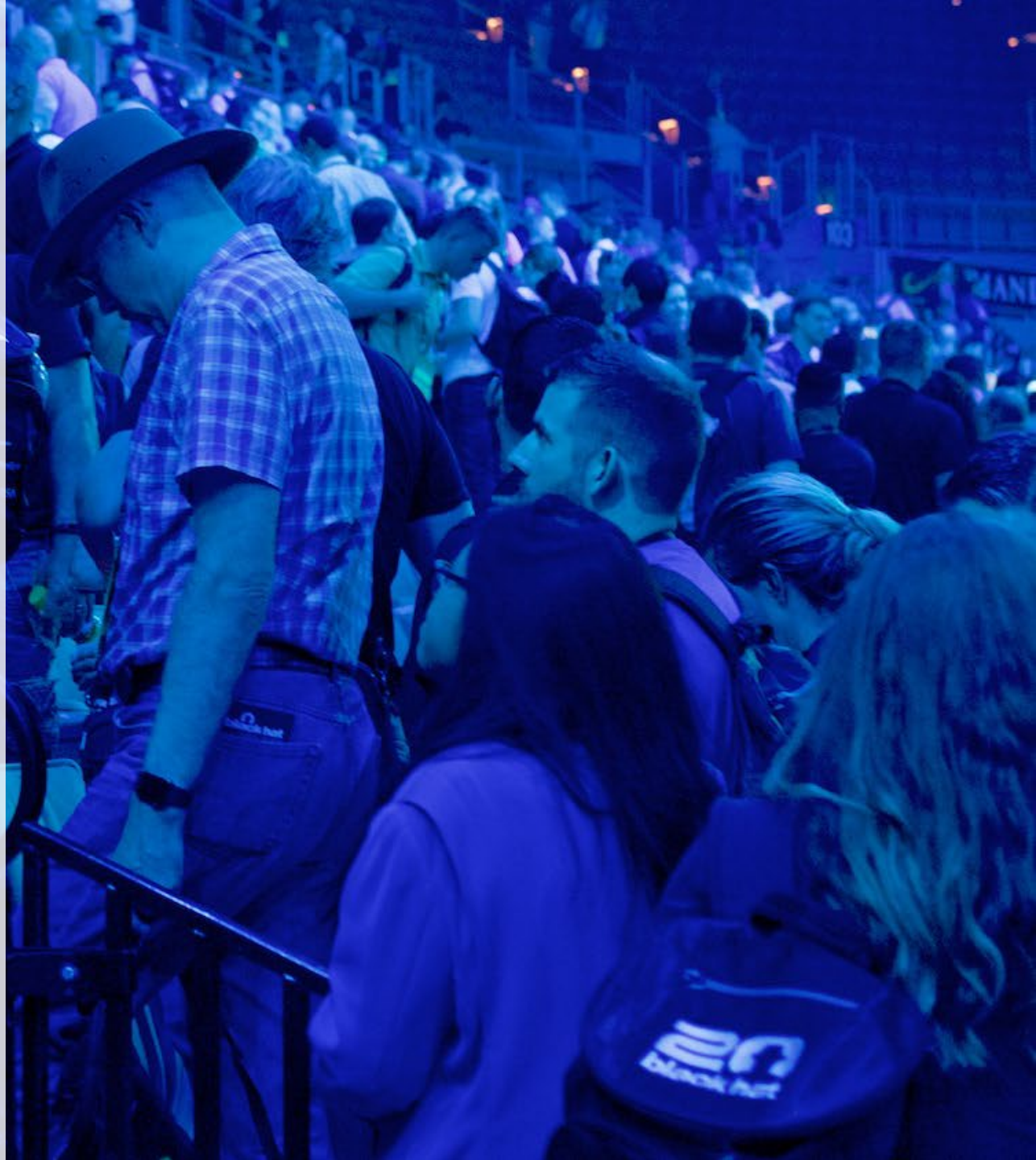
Almost 90% of Cyber Attacks are Caused by Human Error or Behavior

By **Ross Kelly** - March 3, 2017

Few store managers would respond to revelations that a junior assistant had been stealing from the cash register by investing thousands of dollars in new security cameras. It could be far cheaper for them to instill hiring practices that

The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations



MUO

SOCIAL MEDIA, SECURITY

Twitter's New Privacy Policy Means You Need to Change Your Settings

By Nancy Messieh / May 23, 2017 / 3 minutes

Twitter recently **introduced** an updated privacy policy announcing changes to how they collect user data and deliver advertising into your timeline. So what does the update mean and what should you do about it?

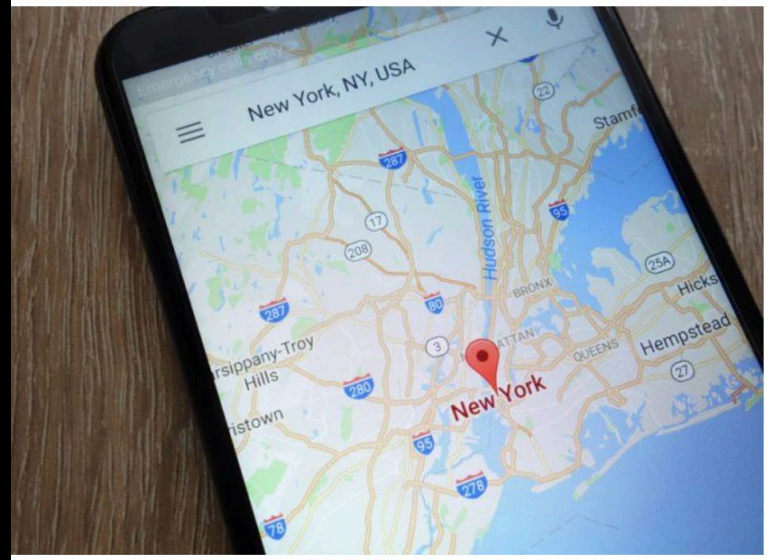
If you haven't logged in to Twitter since the changes were announced, you'll see this message:

ENTERPRISE

Google clarifies its location tracking help page for confused users

by Ellen Tannam

17 AUG 2018 260 VIEWS



Google Maps on mobile device. Image: Piotr Swat/Shutterstock

NEW YORK POST

BUSINESS

Facebook to make privacy settings less difficult to use

By Nicolas Vega

March 28, 2018 | 11:16am

AFP/Getty Images

Facebook said Wednesday it will finally simplify the notoriously confusing maze of privacy settings on its site.

The embattled social network — which previously sent users to more than a dozen different pages when they wanted to adjust the amount of data they shared, or see what third-party apps had access to their information — announced plans to consolidate those settings onto one central page.

Privacy is complicated

Better together

Examining **security/privacy** and **usability** together is often critical for achieving either

USENIX Security 1999

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct

Almost 20 years later Johnny still can't encrypt...

We still rely on users to do security and privacy tasks that they aren’t good at

Creating and remembering unique and complex passwords for dozens of accounts

Comparing crypto key fingerprints

Do they match?

About Our Privacy Policy

Whenever you do something like buy one of our products, watch a show or download an app, information is created. Because we know your privacy is important, we have a Privacy Policy to explain how we collect, use and protect that information. There's a quick summary below, and the actual policy is written in **an easy to understand "Frequently Asked Questions" (FAQ) format (/sites/privacy_policy/terms)**. We want to simplify this explanation, so you can make informed choices about your privacy, and then spend the rest of your time enjoying our products and services.

Effective July 24, 2015

A Quick Summary of Our Privacy Policy

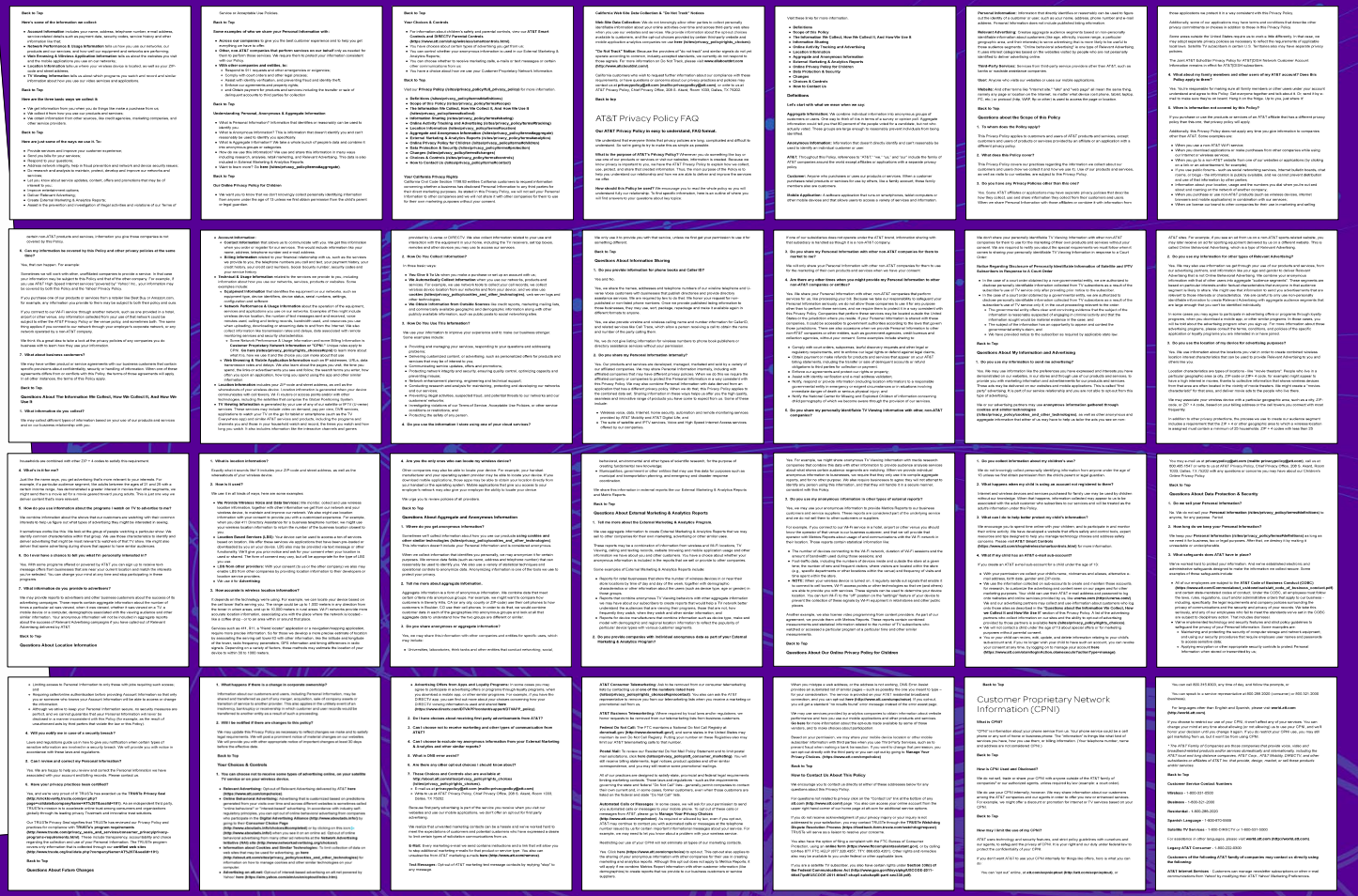
Our Privacy Policy applies to your use of all products, services and websites offered by AT&T and our AT&T affiliates, such as DIRECTV, unless they have a different privacy policy. Because some apps, including some AT&T and DTV branded apps, require additional information, or use information in different ways, they may have their own privacy policies and/or terms and conditions. These apps may also offer you additional choices for managing your personal information.

Back to Top

Our privacy commitments

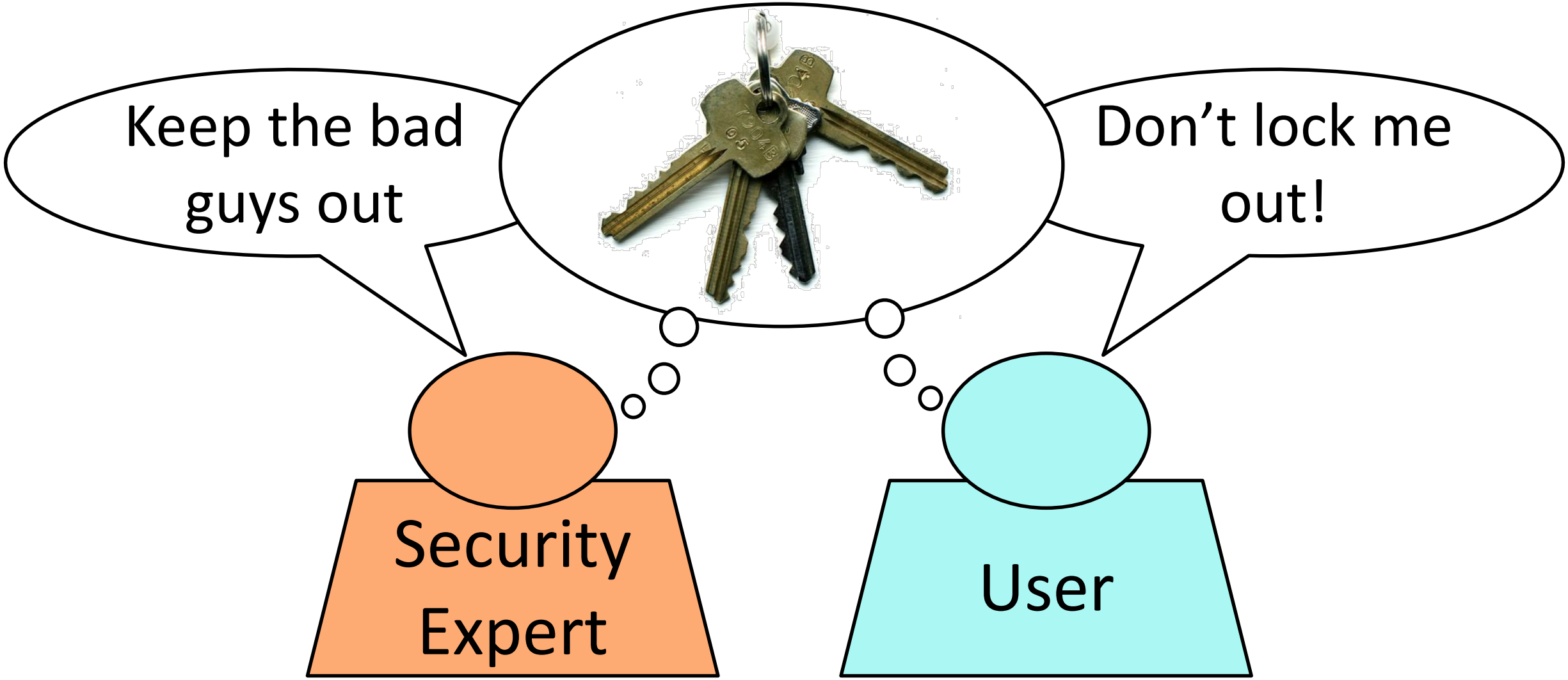
- We don't sell your Personal Information to anyone for any purpose. Period.
- We keep your Personal Information in our business records while you are a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.

Reading and understanding long privacy policies




Security and privacy
are secondary tasks

Concerns may not be aligned



Research on security, privacy, and human behavior

User studies can help us better understand the human threat and design systems that meet user needs

Reasons to conduct user studies

Assess needs

What should we build?

Examine tradeoffs

Which features/approaches best fit particular needs?

Evaluate

Are requirements met?
What should be improved?

Find root causes

What underlying problems need to be fixed?

Excuses for not doing usability studies

- If people weren't so lazy or stupid or careless it would work fine
- I already know what people want
- No time, no money
- I find the system easy to use
- It's so easy my kids can use it
- I'm not a usability expert

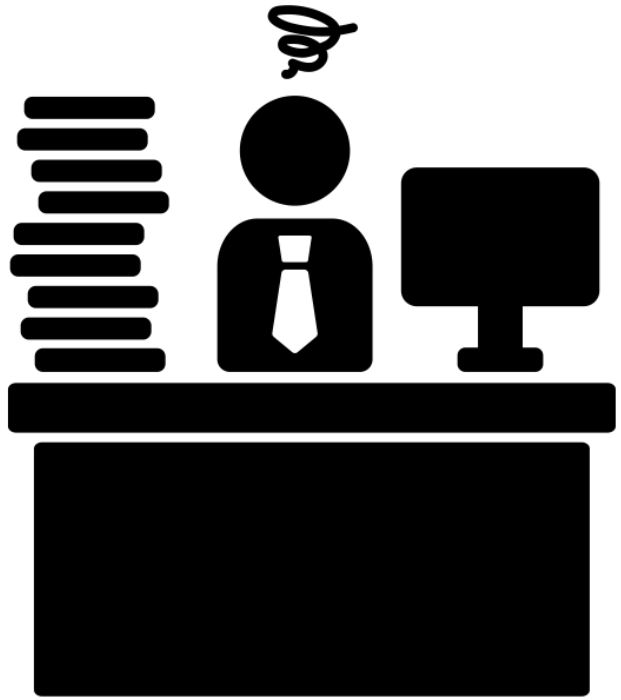
How are security and privacy user studies different from other user studies?

the presence of a **risk/adversary**

simulated

Need to make sure systems are usable and remain secure when…

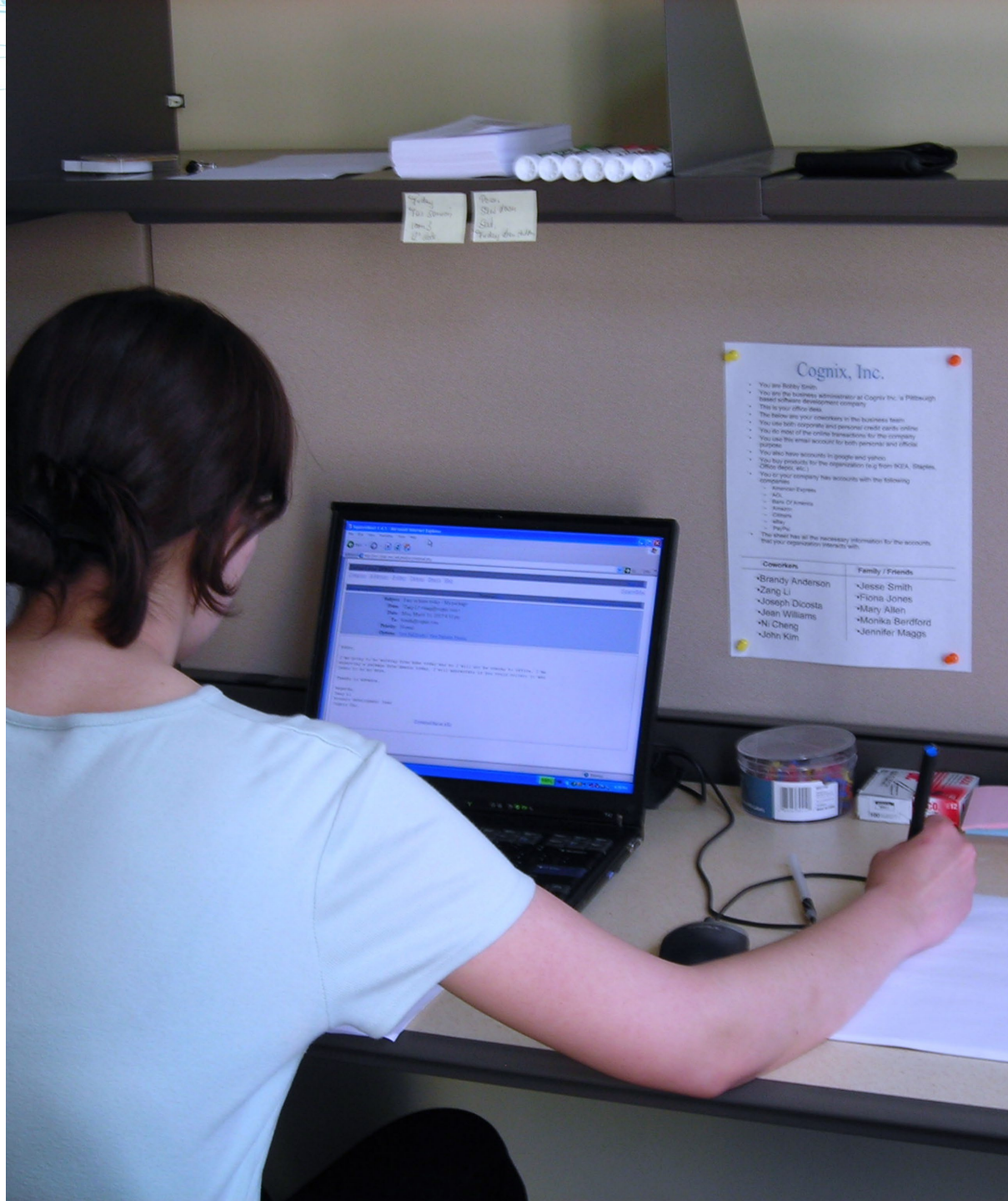
- Attackers (try to) fool users
- Users behave in predictable ways
- Users are unmotivated, careless, stressed, or busy



Icon created by Llisole from Noun Project

Usable security study challenges

- Keeping it real (ecological validity)
- Observing infrequent events and small differences
- Legal, ethical, and practical issues



How can we design a (legal and ethical) study that allows us to observe users in a realistic scenario being exposed to risk?

Self report

- Surveys, interviews, focus groups
  - Opinions
  - Knowledge and perceptions
  - Actions – what have DID or what they WOULD DO in hypothetical situation
- Relatively easy and low cost
- Usually relies on naturally occurring or hypothetical risk
- Relies on people being honest (and remembering accurately)

Survey by Delwar Hossain from the Noun Project

Password perceptions study

B. Ur, J. Bees, S. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? CHI 2016.

`iloveyou88`

`ieatkale88`

Iloveyou88 much more secure

ieatkale88 much more secure

Password perceptions study

B. Ur, J. Bees, S. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? CHI 2016.

`iloveyou88`

`ieatkale88`

Iloveyou88 much more secure

ieatkale88 much more secure

MISCONCEPTION

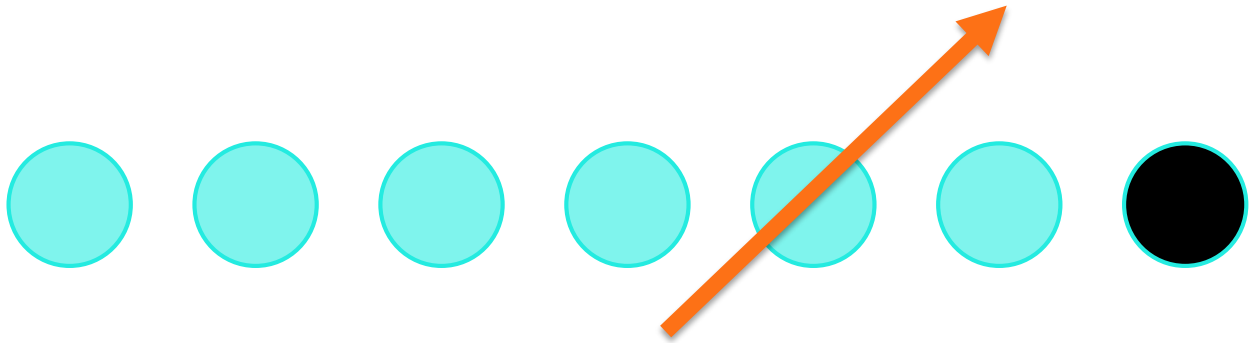
Password perceptions study

B. Ur, J. Bees, S. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? CHI 2016.

`iloveyou88`

`ieatkale88`

Iloveyou88
much more
secure



ieatkale88
much more
secure

4,000,000,000 ×
more secure!

Observe real-world activity

- Many data collection challenges
- Usually not conducive to controlled experiment
- Relies on naturally occurring risk
- Events of interest may be infrequent

Security Behavior Observatory

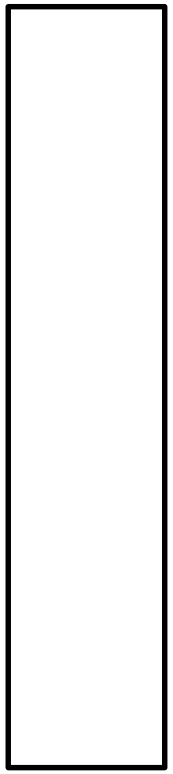
- Network of instrumented home Windows computers
- ~200 active participants
- Natural observation + surveys and interviews
- Data includes hashed passwords

People reuse their passwords a lot

S. Pearman, J. Thomas, P. Emami Naeini, H. Habib, L. Bauer, N. Christin, L. Cranor, S. Egelman, and A. Forget. Let's go in for a closer look: Observing passwords in their natural habitat. CCS 2017.

On average, participants had

- 26 different accounts
- 10 distinct passwords

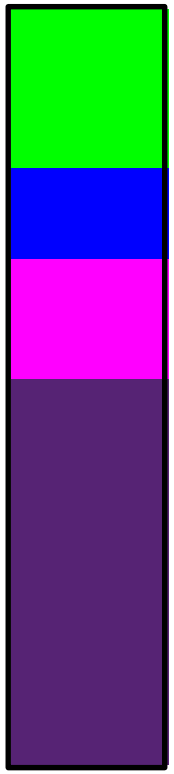


People reuse their passwords a lot

S. Pearman, J. Thomas, P. Emami Naeini, H. Habib, L. Bauer, N. Christin, L. Cranor, S. Egelman, and A. Forget. Let's go in for a closer look: Observing passwords in their natural habitat. CCS 2017.

On average, participants had

- 26 different accounts
- 10 distinct passwords



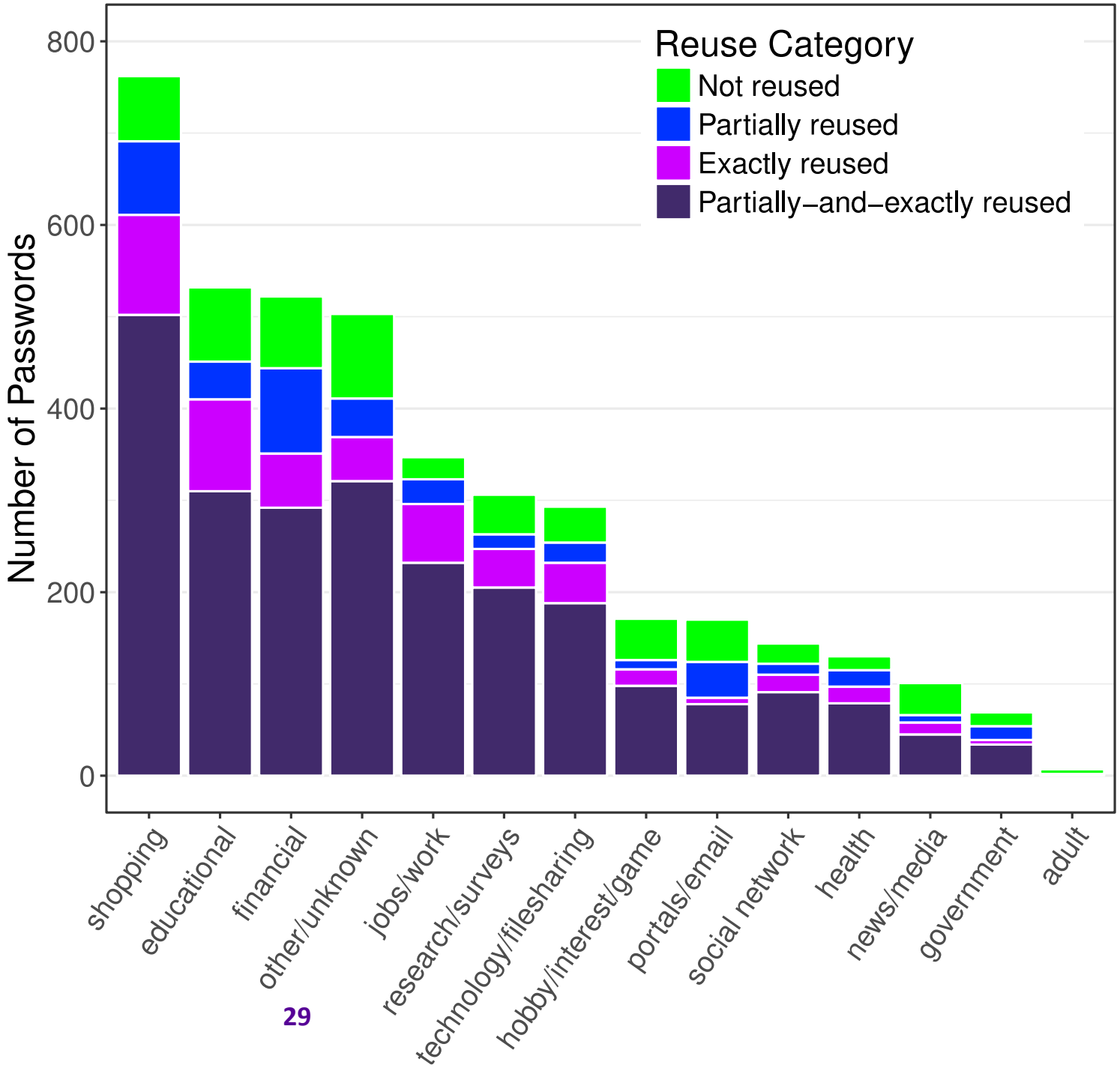
21% Not reused

12% Partially reused

16% Exactly reused

51% Partially and exactly reused

Lots of reuse across almost all categories of websites



Observe hypothetical security tasks

- Ask participants to perform a security task in the context of a hypothetical scenario
- Subject them to ~~real~~ risk

simulated

Not ethical to harm study participants

Observe hypothetical security tasks

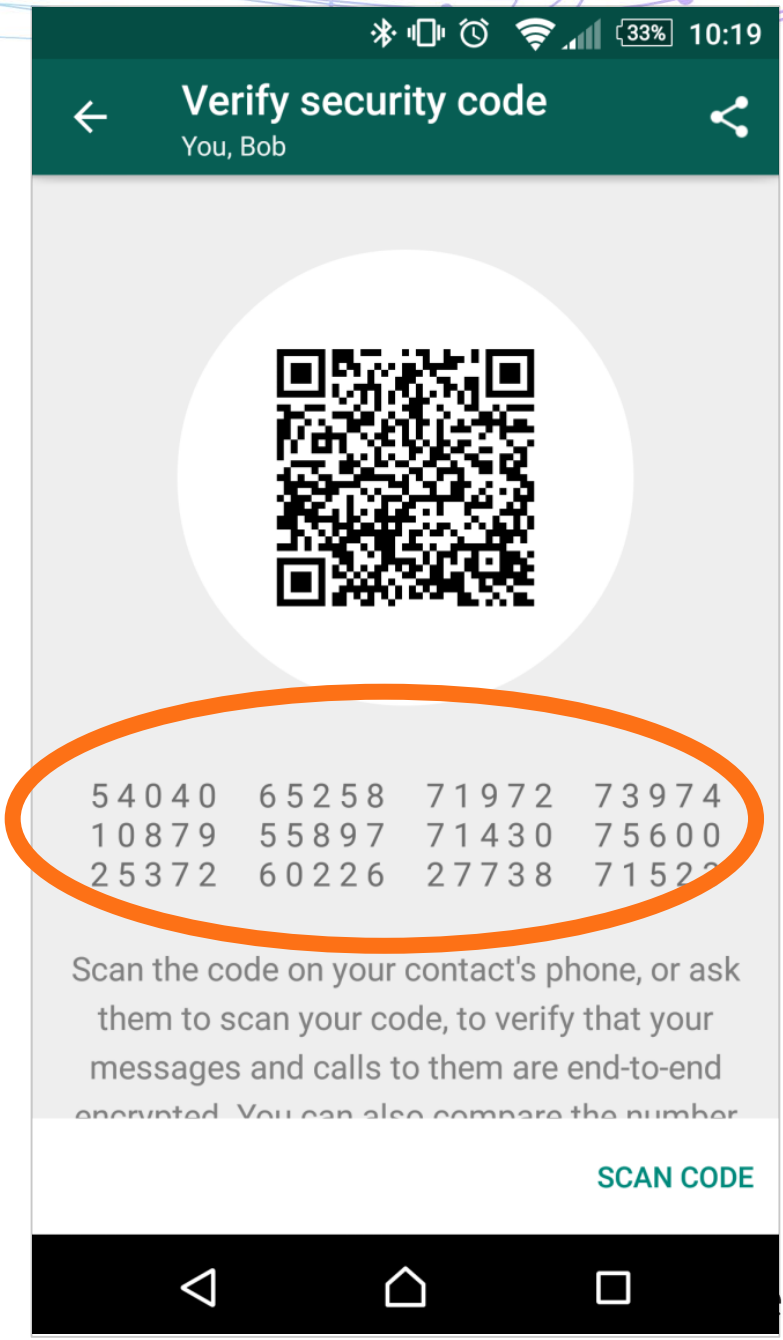
- Ask participants to perform a security task in the context of a hypothetical scenario
- Subject them to ~~real~~ risk

simulated

- May use deception + debrief
- May use economic incentives
- Users may be extra alert to security issues

Alice wants to verify Bob's fingerprint

- WhatsApp provides numeric fingerprints
- Alice can compare this with fingerprint on Bob's business card or other source



What type of fingerprint is best?

```
8174 5886 6247 7685 4281 4047
0930 1306 7201 2113 8177 9827
```

```
+--[ECDSA  256]---+
|         o o.    |
|          = o    |
|         + . .   |
|          o .    |
|         S .     |
|          o E .  |
|           + o +.|
|          . o * +o|
|           o.++*o.|
+-----------------+
```

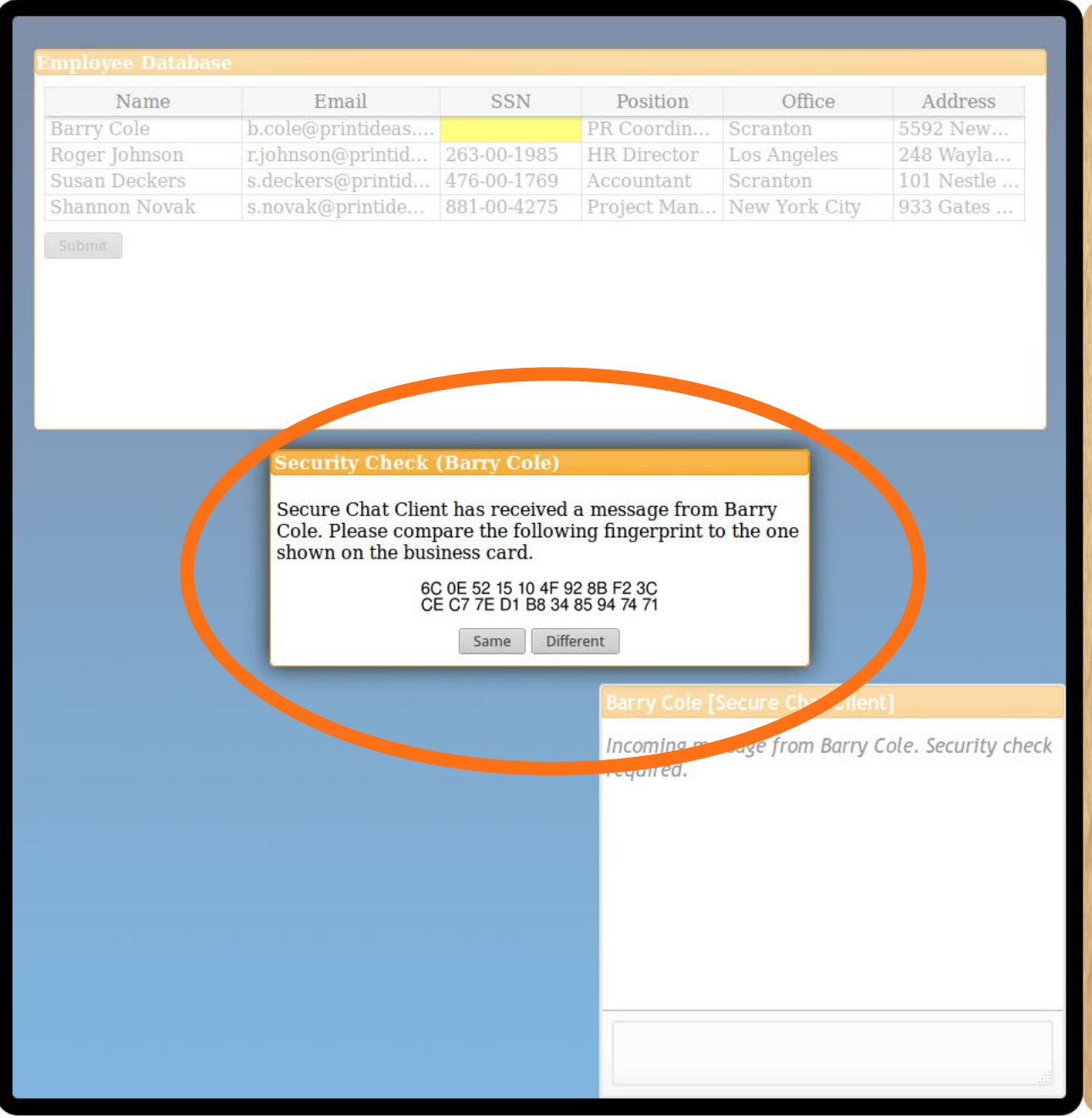
tin yellow blood short attention tax danger bulb wood the normal healthy up false nut bright

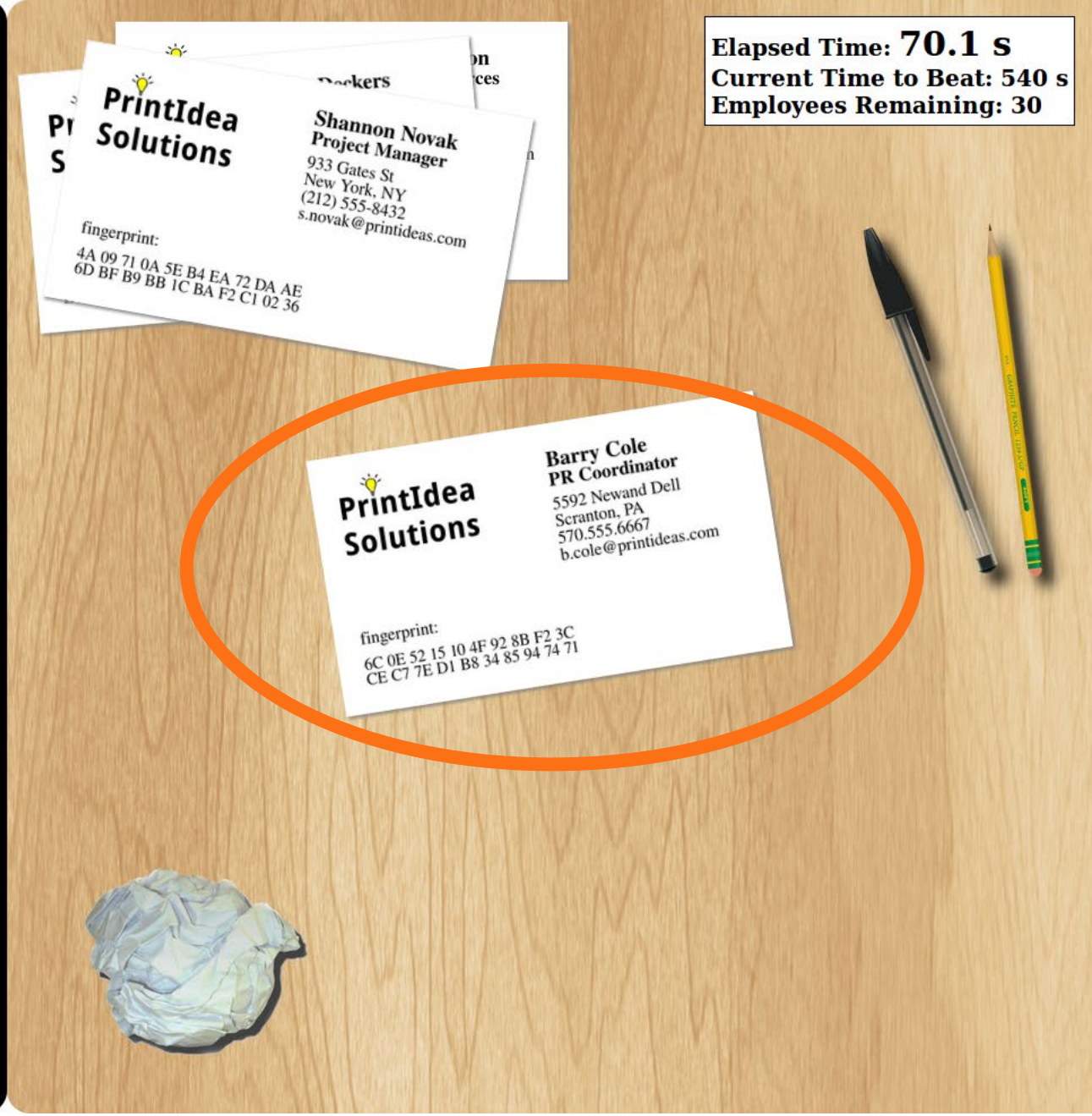
buri padi luya kilo yise rada deyu sipi hofe hage xata rite

Online role-play experiment

Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, Blase Ur. Can Unicorns Help Users Compare Crypto Key Fingerprints? CHI 2017

- 661 participants role-played accountant tasked with updating employee SSNs in database
- For each of 30 employees, required security check involving fingerprint comparison
- Each participant saw 30 fingerprints of same format, **including 1 attack**
- Tested 5 textual formats, 3 graphical formats


Employee Database
Name
Email
SSN
Position
Office
Address
Barry Cole
b.cole@printideas....
PR Coordin...
Scranton
5592 New...
Roger Johnson
r.johnson@printid...
263-00-1985
HR Director
Los Angeles
248 Wayla...
Susan Deckers
s.deckers@printid...
476-00-1769
Accountant
Scranton
101 Nestle ...
Shannon Novak
s.novak@printide...
881-00-4275
Project Man...
New York City
933 Gates ...
Submit
Security Check (Barry Cole)
Secure Chat Client has received a message from Barry Cole. Please compare the following fingerprint to the one shown on the business card.
6C 0E 52 15 10 4F 92 8B F2 3C
CE C7 7E D1 B8 34 85 94 74 71
Same
Different
Barry Cole [Secure Chat Client]
Incoming message from Barry Cole. Security check required.


Elapsed Time: 70.1 s
Current Time to Beat: 540 s
Employees Remaining: 30
PrintIdea Solutions
Shannon Novak
Project Manager
933 Gates St
New York, NY
(212) 555-8432
s.novak@printideas.com
fingerprint:
4A 09 71 0A 5E B4 EA 72 DA AE
6D BF B9 BB 1C BA F2 C1 02 36
PrintIdea Solutions
Barry Cole
PR Coordinator
5592 Newand Dell
Scranton, PA
570.555.6667
b.cole@printideas.com
fingerprint:
6C 0E 52 15 10 4F 92 8B F2 3C
CE C7 7E D1 B8 34 85 94 74 71

People aren’t good at this!

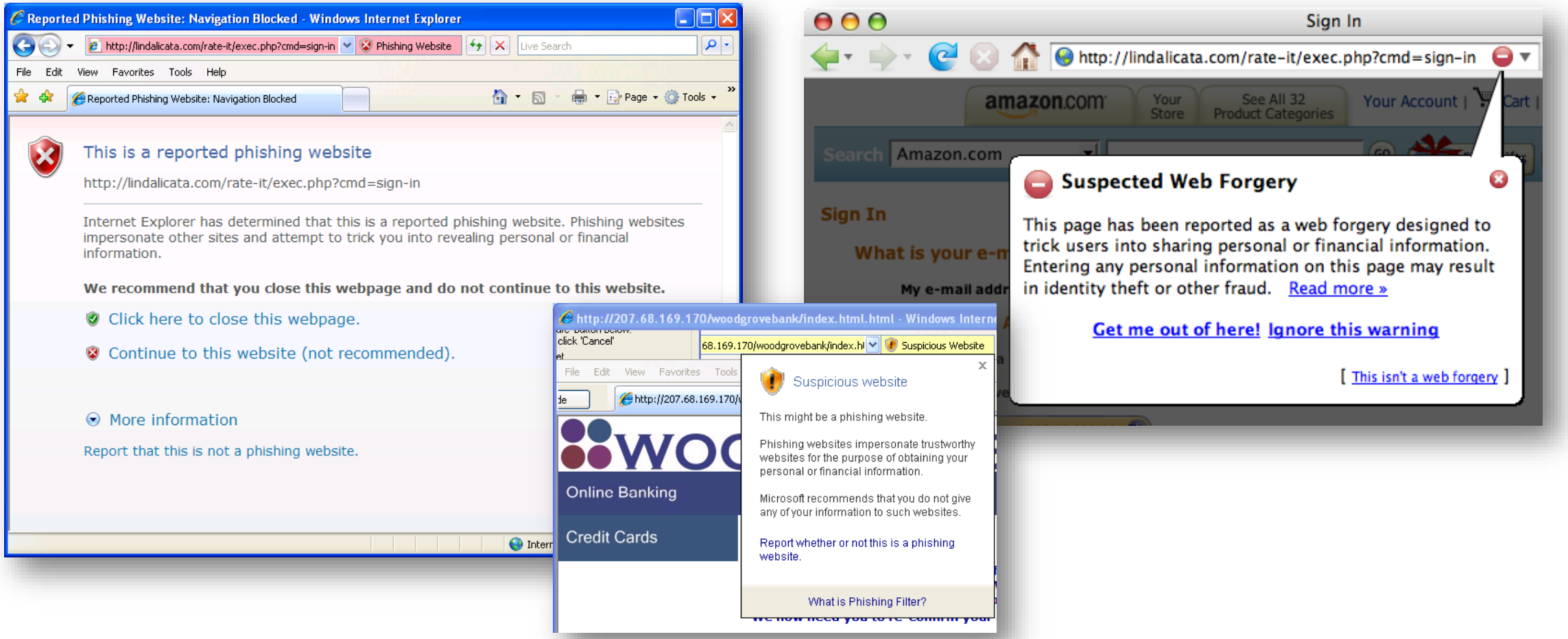
- Textual formats all had similar missed attack rates
- Graphical formats more varied in attack rates, faster to compare
- No fingerprints performed very well
- Unicorn performed the worst!

Observe non-security tasks

- Ask users to perform tasks unrelated to security
- Trigger simulated risk events
- May use deception + debrief

Browser phishing warning study

S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. CHI 2008.



Required a little deception

- Lab study on online shopping
- Purchase paper clips from Amazon
- Answer questions about shopping (for another study)
- That's when we phished them
- Check email to get your receipt
- That's when they fell for it

Your Amazon.com order (#102-6801884-2225735): your approval required Inbox

"Amazon.com" <order-update@amazonaccounts.net> to me show details Jun 13 Reply

Please approve this delay so that we can continue processing your order. (Note that if we haven't received your approval by the end of business tomorrow, the item will be cancelled.

the item will be cancelled. We'll still try to obtain and ship the item(s) before that date.) To do so, visit the following Order Update page in Your Account:

http://www.amazonaccounts.net/gp/signin/104-3310393-0927909.htm

If clicking the above link doesn't work, you can copy and paste the link into your browser's address window, or retype it there.

http://www.amazonaccounts.net/gp/signin/104-3310393-0927909.htm

that cannot accept incoming e-mail. Please do not reply to this message.

Thanks for shopping at Amazon.com, and we hope to see you again.

Sincerely,

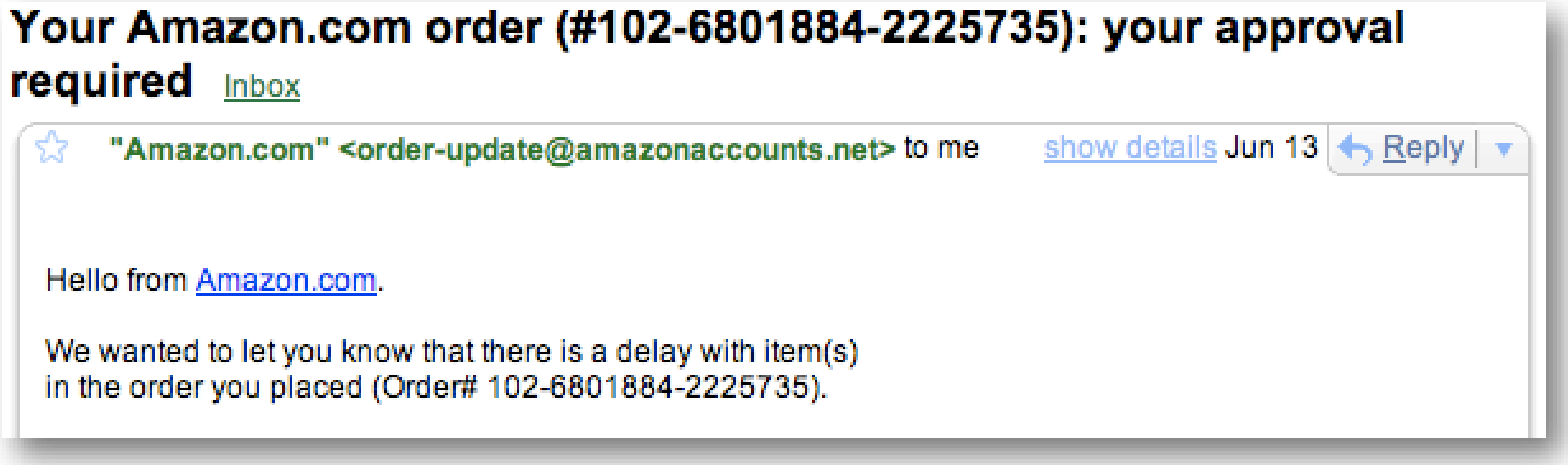
Customer Service Department
http://www.amazon.com
==========
Check your order and more: Order Update

Success!

- Most participants got phished
- Significant differences between conditions
- Observed interesting user behavior that helped us understand root cause of failures

Confused by domain names

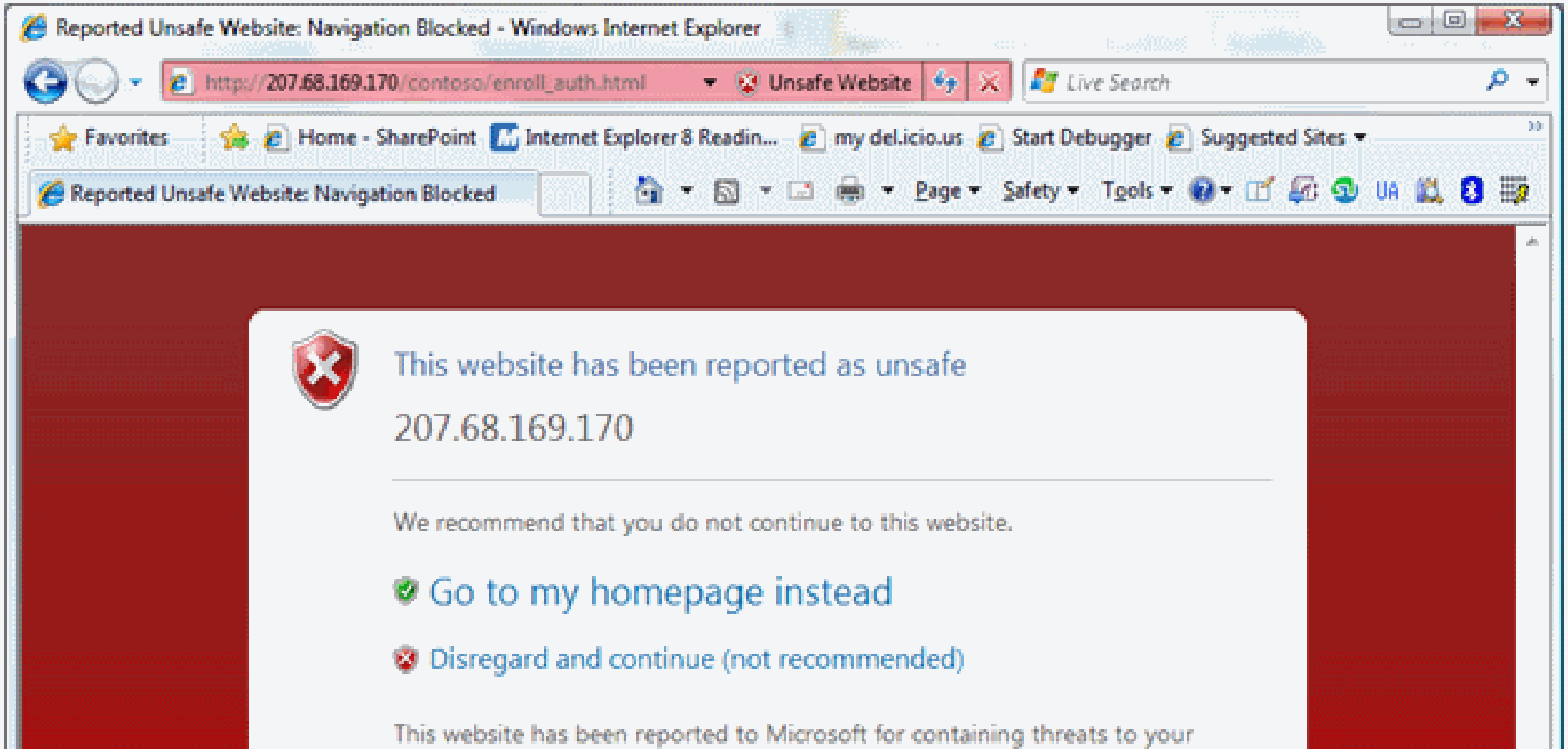
"The address in the browser was of amazonaccounts.net which is a genuine address"



Confused mental models

Some users repeatedly closed their browser, returned to the phishing email, and clicked on the link again

Research led to better phishing warnings



Our agenda today

- Understanding humans
  - 4 talks + discussion
  - Networking break
- Emerging threats
  - 2 talks + discussion
  - Lunch break
- Protecting humans
  - 4 talks + discussion