Lecture 5: Experimental User Studies

CS 181W

Fall 2022

Review: Types of studies

- **Interviews:** conversations with individuals
- **Focus groups:** discussions with groups
- **Surveys:** asynchronous questions

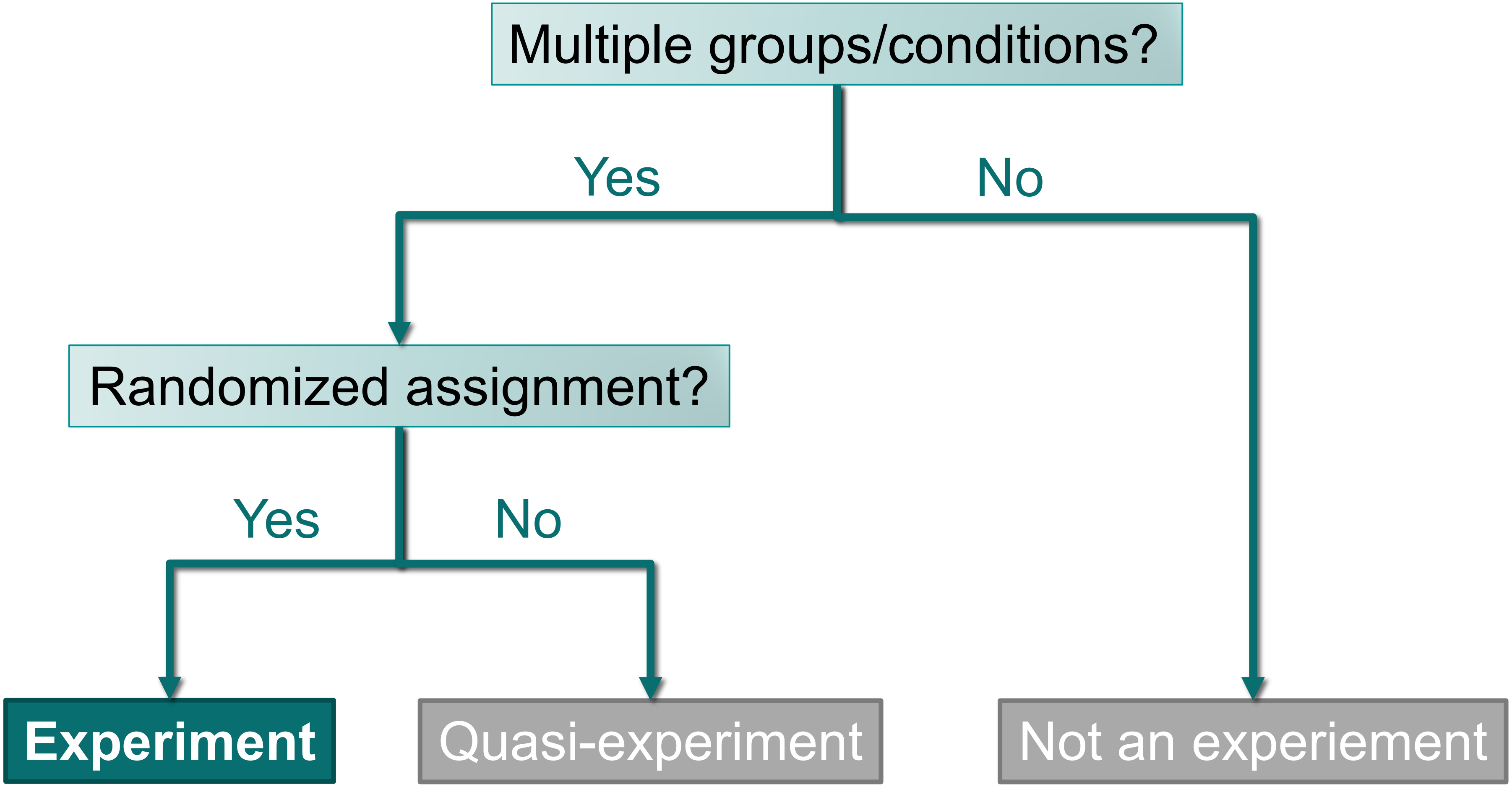
- **Experimental Studies:** randomized multi-condition studies
- **Usability Testing:** observations of tool use
- **Cognitive Walkthrough:** expert evaluation

- **Diary Studies:** contemporary record of real-world behavior
- **Observational Studies:** records of behavior in the wild

- Mixed-methods studies

EXPERIMENTAL STUDIES

What is an experimental study?



Why do an experimental study?

- Observe how people behave in various circumstances
- Test hypotheses about and identify causal relationships
- Can evaluate designs and tools that do not yet exist
- Large-scale experiments (can be) representative of population

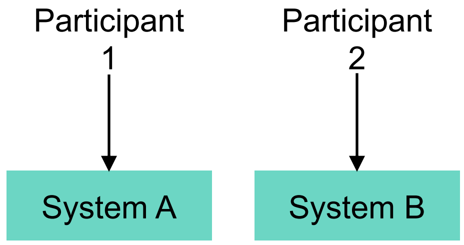
Experimental Study Limitations

- Ecological Validity: extent that experimental setup mirrors real-life conditions and context

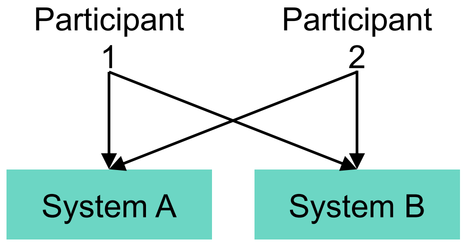
- External Validity: extent to which we can generalize about our results

Study designs

- Between subjects
  - Each participant tests 1 version of the system
  - You compare these groups
  - Randomize!
  - Groups should be similar (verify!)



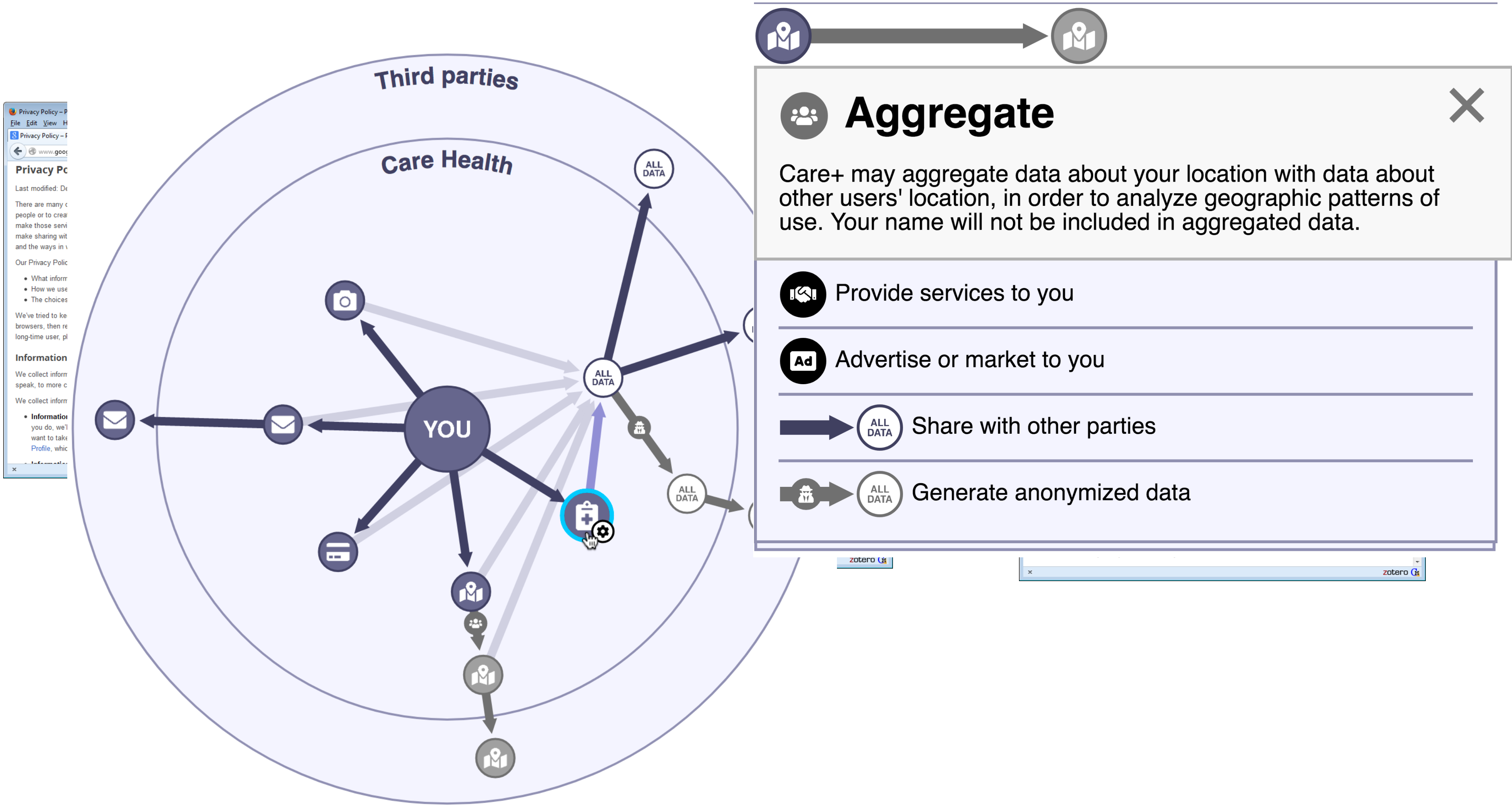
- Within subjects
  - Every participant tests everything
  - Fewer participants
  - Crucial to randomize order! (learning effect)



Data to collect during experiments

- Performance (time, success rate, errors)
- Actions and decisions
  - Think-aloud, audio, screen capture, video, mouse movements, keystrokes
- Opinions, preferences, and attitudes
- Demographics
  - Age, gender, technical background, income, education, occupation, location, disabilities, first language, privacy attitudes, etc.

Example: Usability Experiment



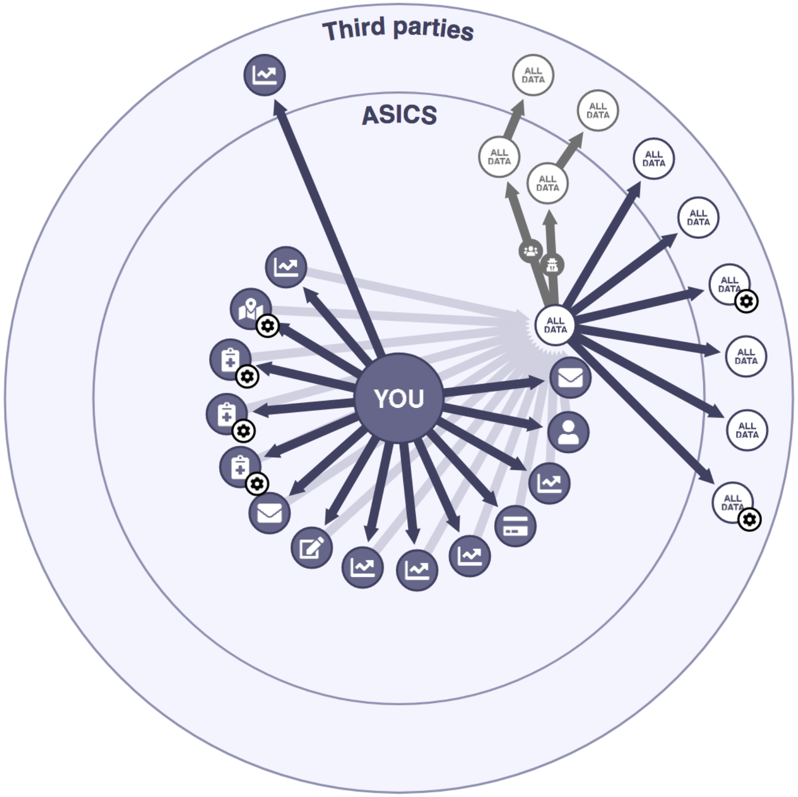
Aggregate

Care+ may aggregate data about your location with data about other users' location, in order to analyze geographic patterns of use. Your name will not be included in aggregated data.

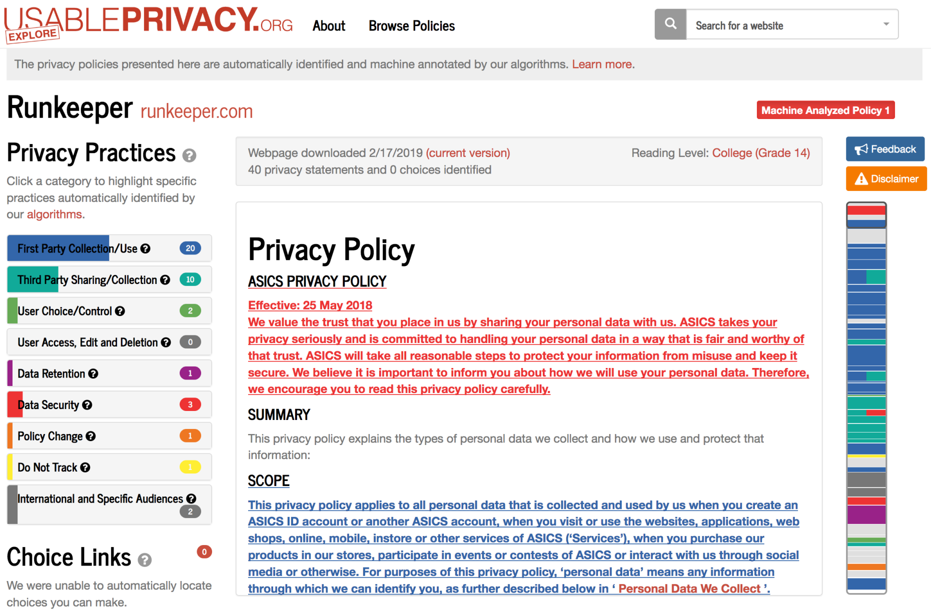
- Provide services to you
- Advertise or market to you
- ALL DATA Share with other parties
- ALL DATA Generate anonymized data

Example: Usability Experiment

Poli-See



Annotated Privacy Policies



The privacy policies presented here are automatically identified and machine annotated by our algorithms. Learn more.

Runkeeper runkeeper.com

Privacy Practices

Click a category to highlight specific practices automatically identified by our algorithms.

First Party Collection/Use	20
Third Party Sharing/Collection	10
User Choice/Control	2
User Access, Edit and Deletion	0
Data Retention	1
Data Security	3
Policy Change	1
Do Not Track	1
International and Specific Audiences	2

Choice Links 0

We were unable to automatically locate choices you can make.

Webpage downloaded 2/17/2019 (current version) Reading Level: College (Grade 14)
40 privacy statements and 0 choices identified

Privacy Policy

ASICS PRIVACY POLICY

Effective: 25 May 2018

We value the trust that you place in us by sharing your personal data with us. ASICS takes your privacy seriously and is committed to handling your personal data in a way that is fair and worthy of that trust. ASICS will take all reasonable steps to protect your information from misuse and keep it secure. We believe it is important to inform you about how we will use your personal data. Therefore, we encourage you to read this privacy policy carefully.

SUMMARY

This privacy policy explains the types of personal data we collect and how we use and protect that information:

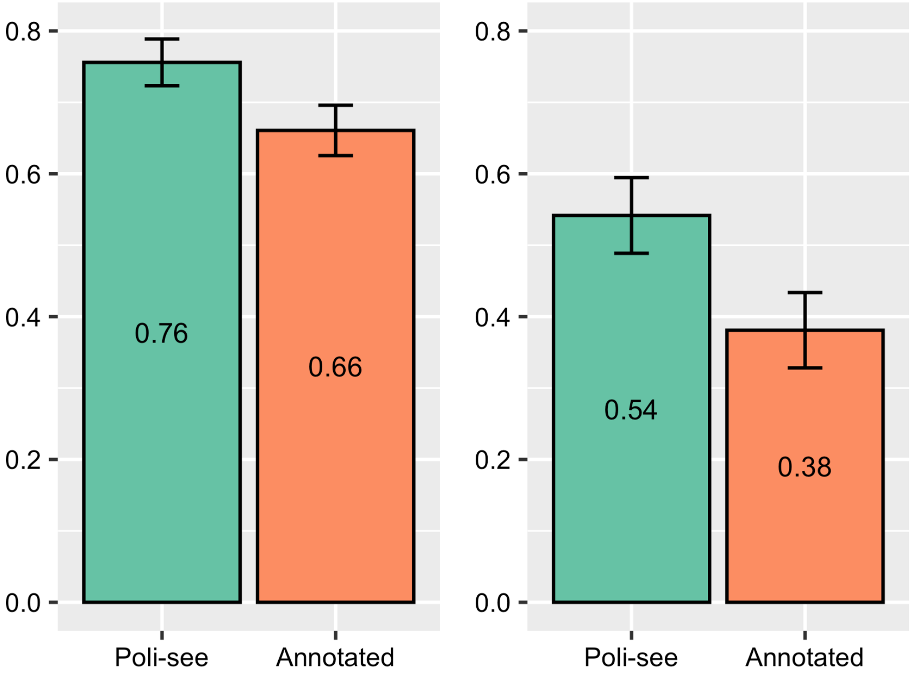
SCOPE

This privacy policy applies to all personal data that is collected and used by us when you create an ASICS ID account or another ASICS account, when you visit or use the websites, applications, web shops, online, mobile, instore or other services of ASICS ('Services'), when you purchase our products in our stores, participate in events or contests of ASICS or interact with us through social media or otherwise. For purposes of this privacy policy, 'personal data' means any information through which we can identify you, as further described below in ' Personal Data We Collect '.

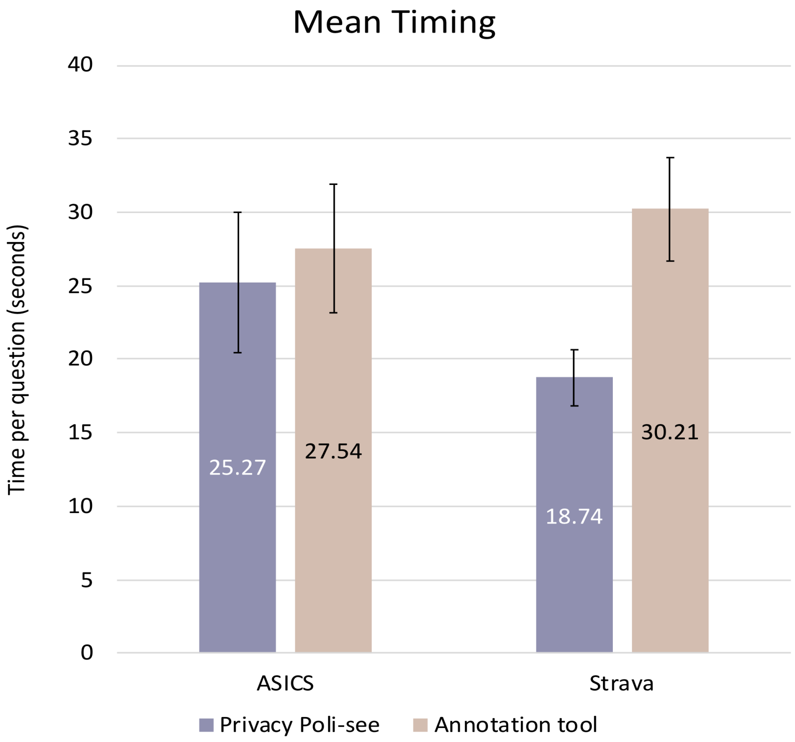
24 participants
In-lab
Within subject

Example: Usability Experiment

Performance (Accuracy)

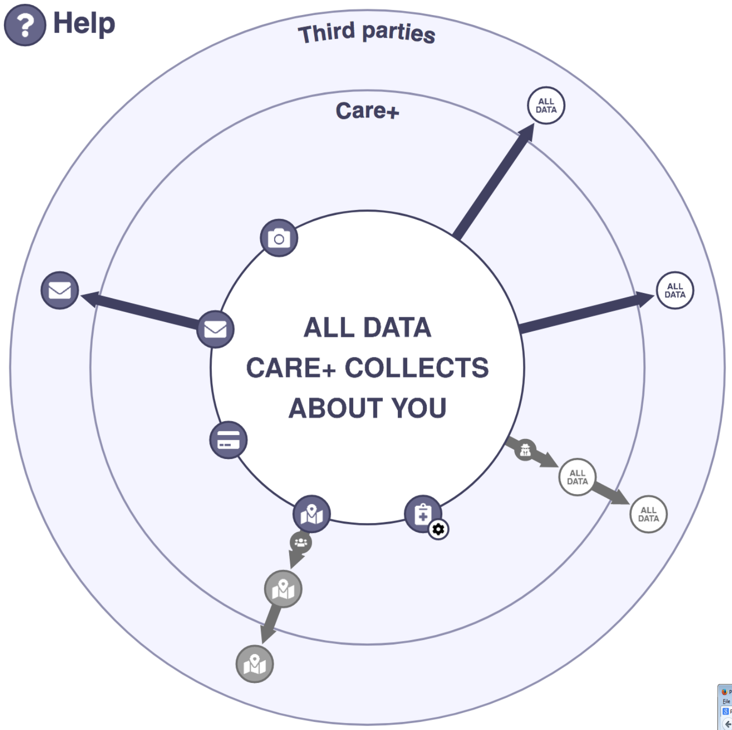


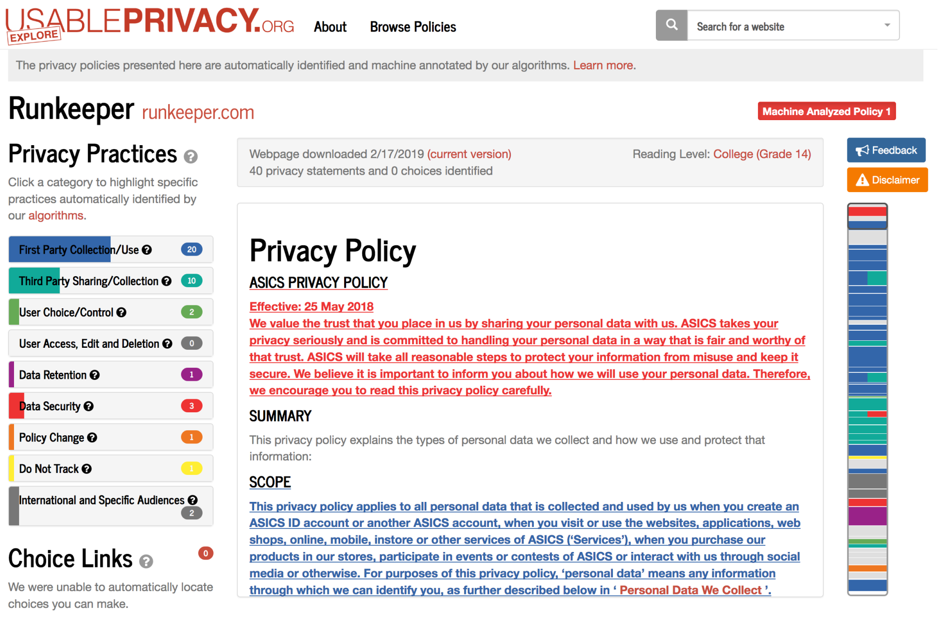
Other Measurements



> “the picture really helped me, and you could just go round in a circle; it was kind of fun.”

Example: Usability Study 2




USABLEPRIVACY.ORG EXPLORE About Browse Policies Search for a website

The privacy policies presented here are automatically identified and machine annotated by our algorithms. Learn more.

Runkeeper runkeeper.com

Machine Analyzed Policy 1

Privacy Practices

Click a category to highlight specific practices automatically identified by our algorithms.

First Party Collection/Use	20
Third Party Sharing/Collection	10
User Choice/Control	2
User Access, Edit and Deletion	0
Data Retention	1
Data Security	3
Policy Change	1
Do Not Track	1
International and Specific Audiences	2

Choice Links 0

We were unable to automatically locate choices you can make.

Webpage downloaded 2/17/2019 (current version)
40 privacy statements and 0 choices identified

Reading Level: College (Grade 14)

Feedback

Disclaimer

Privacy Policy

ASICS PRIVACY POLICY

Effective: 25 May 2018

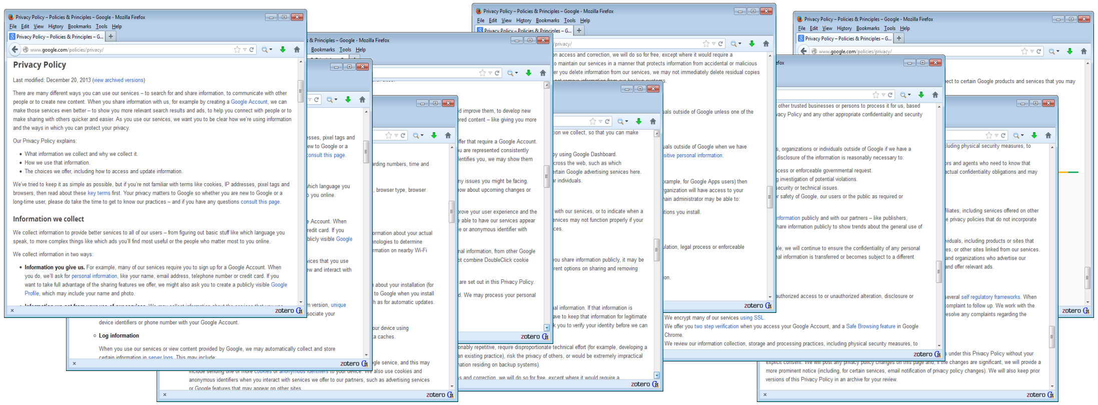
We value the trust that you place in us by sharing your personal data with us. ASICS takes your privacy seriously and is committed to handling your personal data in a way that is fair and worthy of that trust. ASICS will take all reasonable steps to protect your information from misuse and keep it secure. We believe it is important to inform you about how we will use your personal data. Therefore, we encourage you to read this privacy policy carefully.

SUMMARY

This privacy policy explains the types of personal data we collect and how we use and protect that information:

SCOPE

This privacy policy applies to all personal data that is collected and used by us when you create an ASICS ID account or another ASICS account, when you visit or use the websites, applications, web shops, online, mobile, instore or other services of ASICS ('Services'), when you purchase our products in our stores, participate in events or contests of ASICS or interact with us through social media or otherwise. For purposes of this privacy policy, 'personal data' means any information through which we can identify you, as further described below in ' Personal Data We Collect '.


Privacy Policy – Policies & Principles – Google - Mozilla Firefox

Privacy Policy

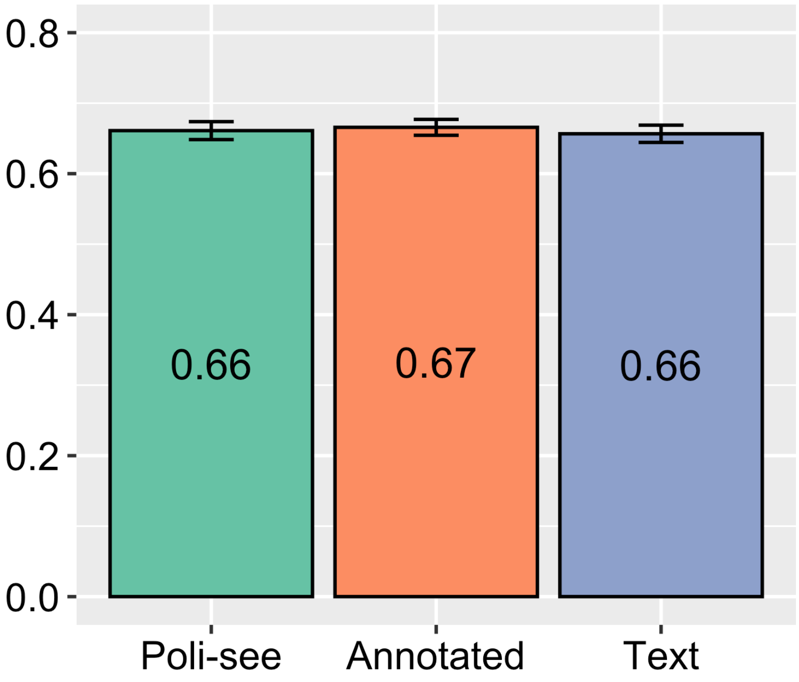
Last modified: December 20, 2013 (view archived versions)

Information we collect

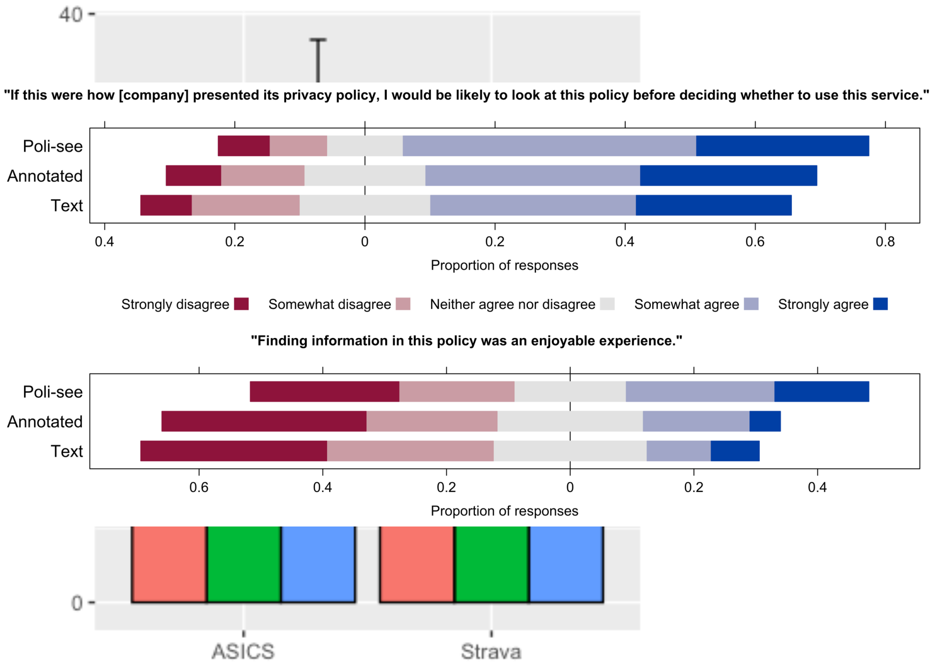
600 participants
Online
Between subjects

Example: Usability Study 2

Performance (Accuracy)



Other Measurements



Exercise: Usability Studies

- Google implements Right to Access with a tool called Google takeout
- Design a usability study OR usability experiment that would evaluate this tool

- Things to consider:
  - What conditions would you have (if any)?
    - If have multiple conditions, within subject or between subjects?
  - What tasks would your participants complete?
  - What data would you collect?
  - Would you conduct this study in person ("lab") or online?

Usable security study challenges

- Keeping it real (ecological validity)
  - the presence of a **risk/adversary**

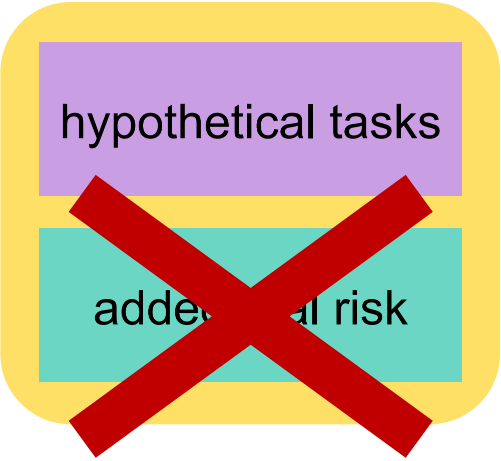
    ^
    simulated

- 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?

Designing Experiments with Risk



Not ethical to harm study participants

Designing Experiments with Risk

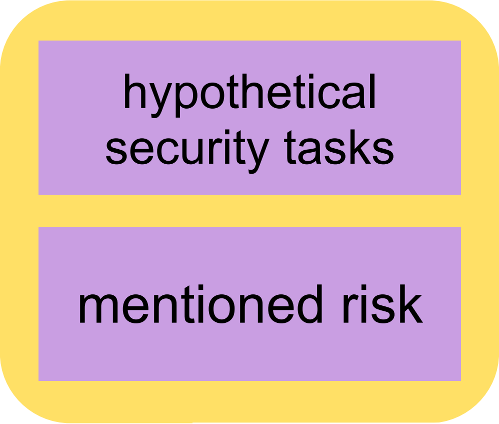
Real World Activity

observation of real-world activity

naturally-occurring risk

- Usually not conducive to a controlled experiment
- Events of interest may be infrequent
- Many data collection challenges
- More on this on Wednesday!

Simulated Risk


hypothetical security tasks

mentioned risk

Background: Encryption

Symmetric Encryption

- e.g., AES
- Pros: fast, works on arbitrary-length messages
- Cons: need n^2 keys, key distribution

Asymmetric (Public-key) Encryption

- e.g., RSA
- Pros: only need one key
- Cons: (very!) slow, key authentication

Hybrid Encryption: generate fresh AES key each time, use other person's public key to encrypt AES session key and send it to them

Authenticating Keys

Decentralized Approach

- Users distribute keys to other people who need to contact them

Centralized PKI Infrastructure

- Certificate authorities (CAs) sign digital certificates asserting that certain public keys belong to certain principals
- Certificate chains
- You decide which CAs you trust

Secure messaging

- Private communications tools
- Sender needs to reliably obtain recipient's public key to send an encrypted message
- Important to check to make sure you have correct key

WhatsApp

Signal Private Messenger

GnuPG

Public key → fingerprint

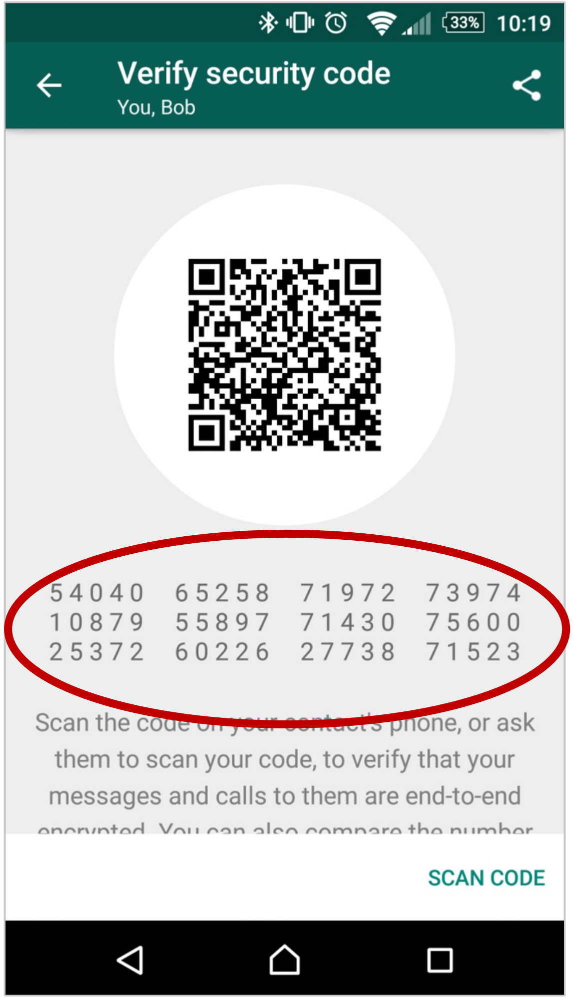
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.5
Comment: Hostname: pgp.mit.edu

mQINBFLsrT0BEADI72WmFPt4Q8+3zhtXfxg7MtIilamR0XLk0CSy5jEJk38rLb6Sxr7TCHD1
sD/W/Iy8atV3UA5MUwTZ12iU08MAGW49qmEp9atY7alFtL2p1mGBV0nd8gx0nuLFstGaFIUv
WRVlmeRxiU5zneH2Slt+dgjDsUWMN4nFNnP+87FMI98Q82OdwDai7hXtGKaxLYpzIo9gfFGy
W2x47FXvMxQTC4pUyavkKsv4Q9qfx4cS/Bxv5eezNn/O76b47L/xwJOgCUJILt4udig7RYyI
y8Y0wO5cBwVIfd/XzIig7q0vzEgVCLFnhghyJsguLMjRXa/pCuCAiNkeiqHHwdT3GRHSbGh+
SsUJ6JUcj5nzh5ODpExEGDv1wlncE7DIpwpxM+ct4muVMYqhe6moP6rsOa/aTi+3Jw+Hg80n
FsKlpizCUsAtTFft94tOFZw+uplu+AGPZ8qD1J490V5GZo+7RkUFYxNq/Zt0GAcB+KaW4MTZ
CpDBUJRAnWm/k/n0OYbdjQsTR/Si7cnkLFhQMRN3yaETLsE0WKUYBBmJPug7bhkDEWkF15MJ
dF1N5EQ7Hb1tlFi39zYBhZYMkYEaVviRYAPlVQLOCzVSsS4xUyivRsDRmSX7DLmaW8tY1NwE
8QvJ6mjNQy+V/DdSQf9cMdVu7NMnk8Cb5HOuEgjl9wywm4wWgQARAQABtB5Kb3NodWEgVGFu
IDxqdGFuMTg5QGdtYWlsLmNvbT6JAj0EEwEKACcFAlLsrT0CGwMFCQHhM4AFCwkIBwMFFQoJ
CAsFFgIDAQACHgECF4AACgkQiZDZY75OwYzPaA//aH6+4lN6d1egxPG+NDzcaCPv73gbIxtZ
u19fi9WtVAnLBqGykOHL1Yw+hCH9jFWYfRq8vmiRaRuVQn/7Wf+JcsQway2M7XICeOEg2bPv
uR3eQ50jYyvqEkxSgzoBRp46aSm/9S1wHvwp62C5Hu3Cnjlvb/vFQgWB4tfuyVVjqcpn//Qv
0Jas5SZ6TUid6yLpkFq8U1AQo24Wl2Ns8pfXJoUAfeL0fUoDoQ++0t1V7Zsog7sOIxVXfEyk
…
```

```
C6C2 78B5 6F92 2B8F 5A07
5B17 69F5 2C6E F103 4425
```

Key → Fingerprint

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



Verify security code

You, Bob

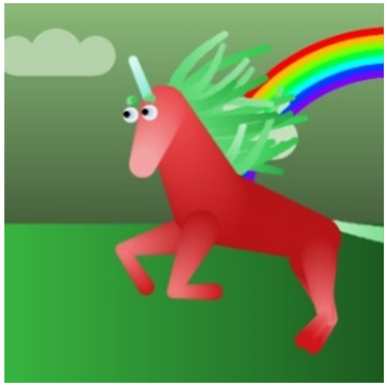
```
54040 65258 71972 73974
10879 55897 71430 75600
25372 60226 27738 71523
```

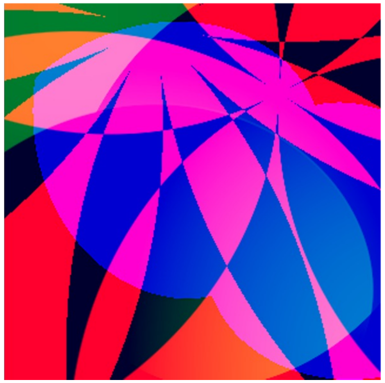
Scan the code on your contact's phone, or ask them to scan your code, to verify that your messages and calls to them are end-to-end encrypted. You can also compare the number

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

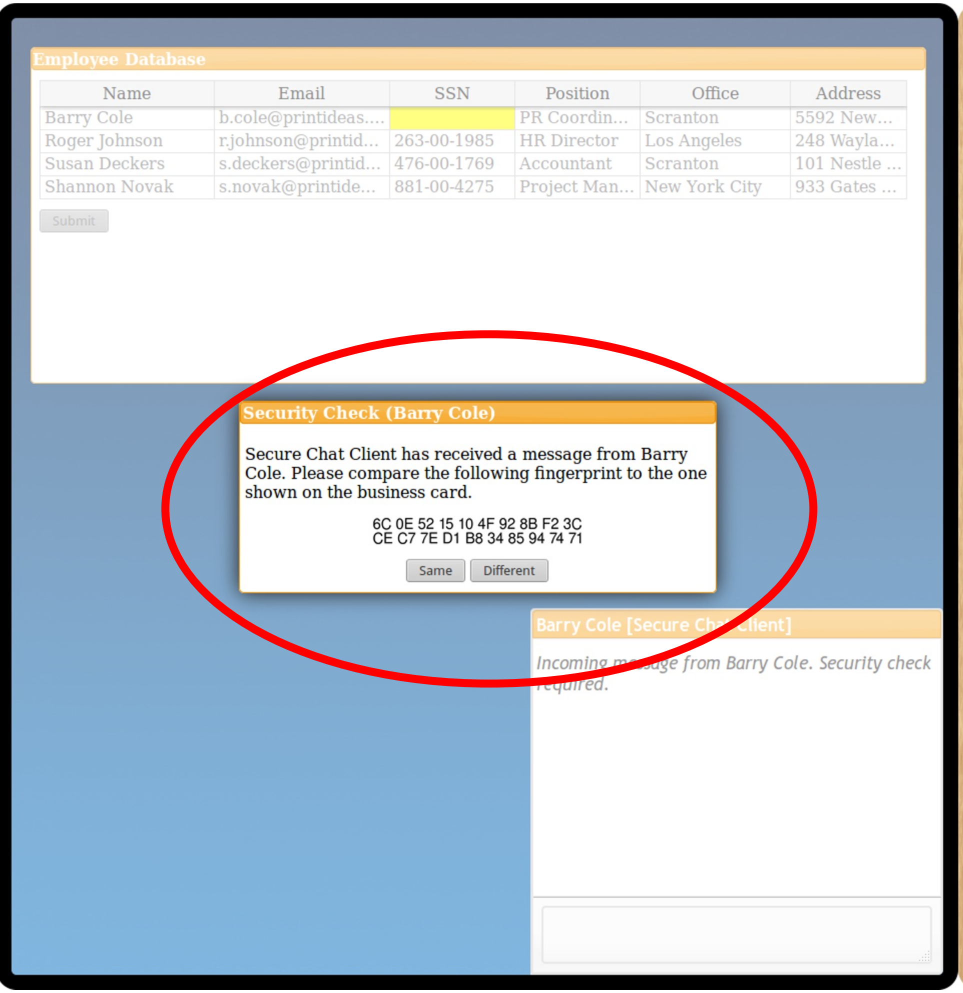
buri padi luya kilo yise rada deyu sipi hofe hage xata rite

```
C6C2 78B5 6F92 2B8F 5A07
5B17 69F5 2C6E F103 4425
```

661 participants
Online
Between subjects

661-participant Mturk experiment

- 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 text formats, 3 graphical formats
- Monetary incentive for finishing quickly and securely



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 ...

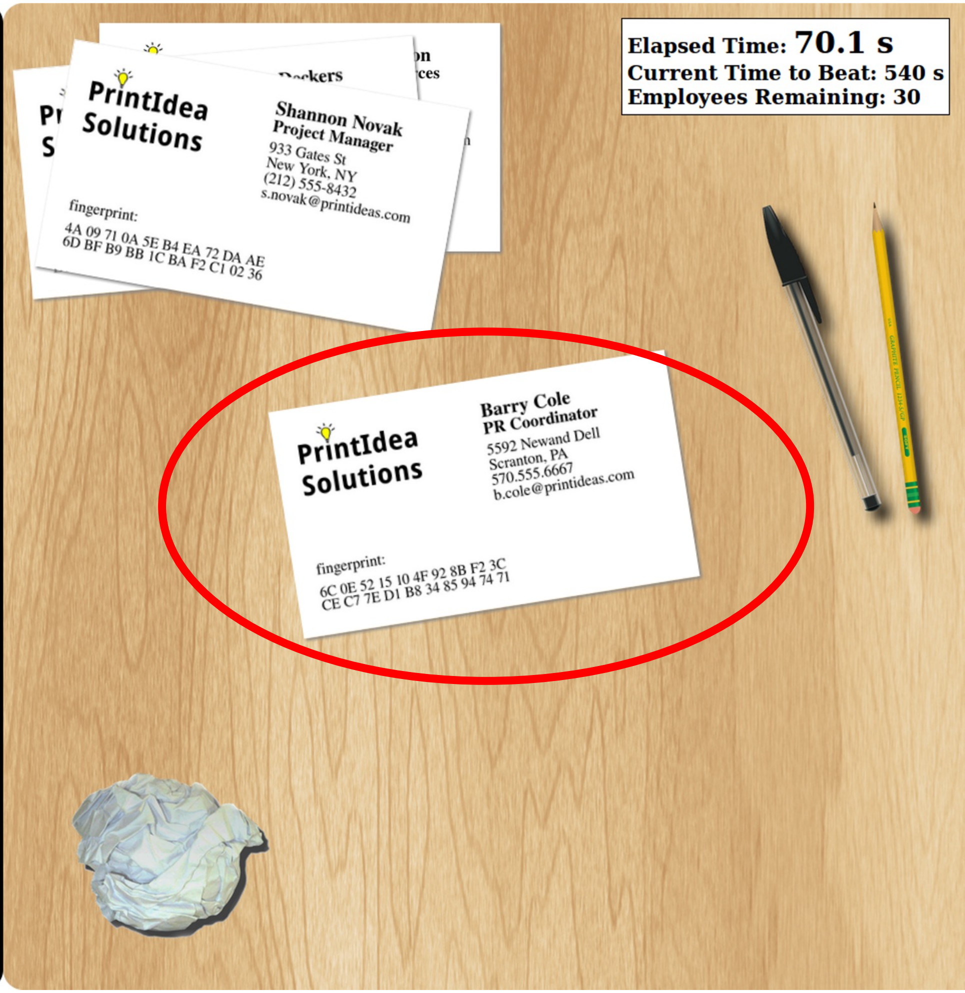
Security Check (Barry Cole)

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

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

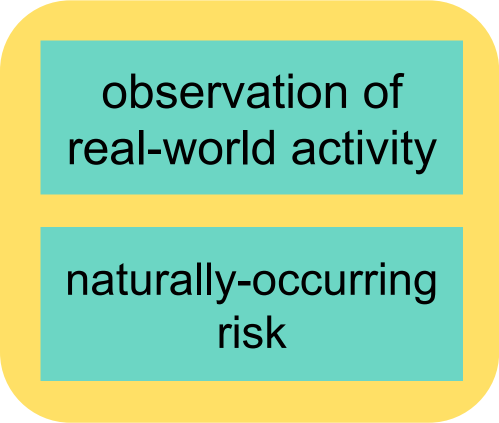
fingerprint:
6C 0E 52 15 10 4F 92 8B F2 3C
CE C7 7E D1 B8 34 85 94 74 71

Results: people aren’t good at this!

- Textual formats all had similar missed attack rates
- Graphical formats more varied in attack rates, faster to compare
- Most attacks missed in unicorn condition
- No fingerprints performed very well

Designing Experiments with Risk

Real World Activity

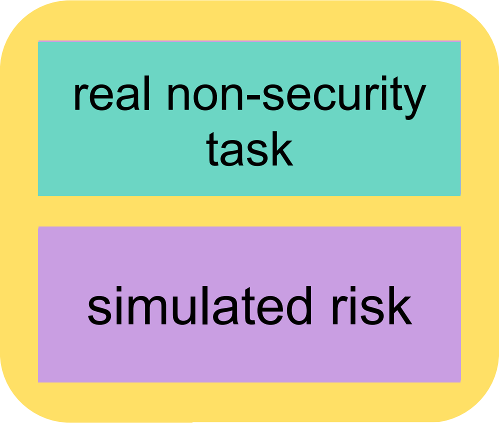


observation of real-world activity

naturally-occurring risk

- Usually not conducive to a controlled experiment
- Events of interest may be infrequent
- Many data collection challenges
- More on this on Wednesday!

Simulated Risk



real non-security task

simulated risk

Authenticating Keys

Decentralized Approach

- Users distribute keys to other people who need to contact them

Centralized PKI Infrastructure

- Certificate authorities (CAs) sign digital certificates asserting that certain public keys belong to certain principals
- Certificate chains
- You decide which CAs you trust

SSL certificate warnings

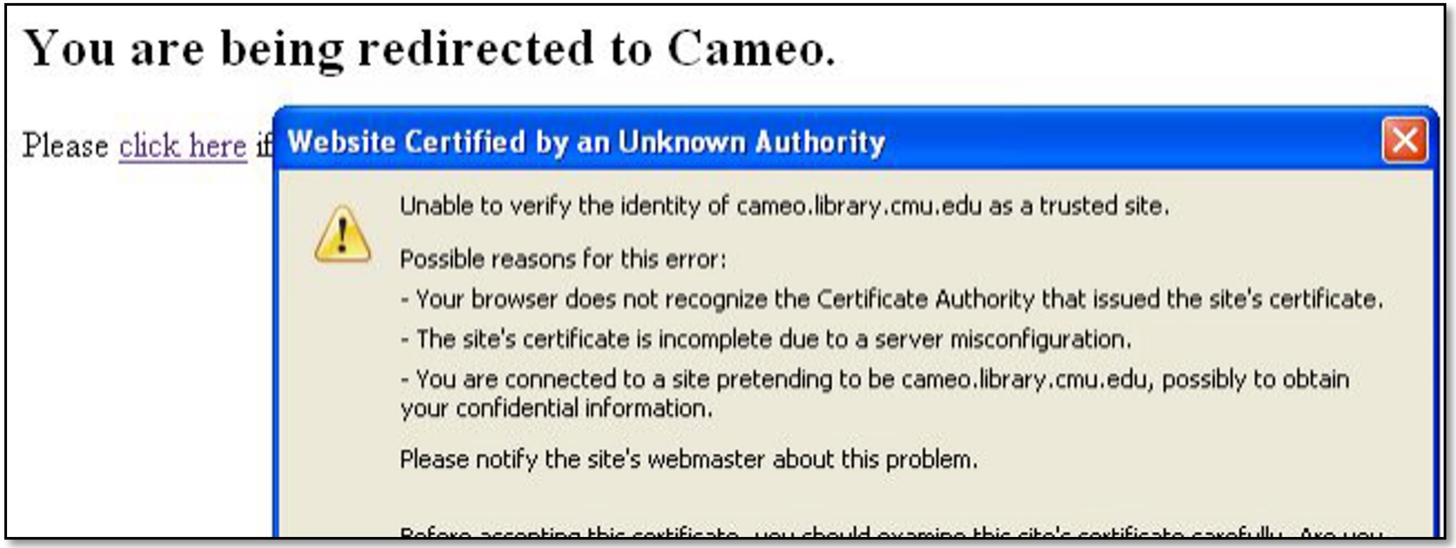
- Browsers warn about SSL Cert problems:
  - Domain Mismatch
  - Unknown Certificate Authority
  - Expired
- These warnings
  - May be user’s only protection
  - Commonly encountered when connecting to legitimate servers

A good warning helps users determine whether they are at risk

- Stops users from doing something dangerous in risky context
- Doesn’t interfere with non-risky contexts
- Need to test warnings in both contexts

Non-risky context

- Visit CMU “Cameo” library web site
- Encounter self-signed certificate (familiar experience)



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

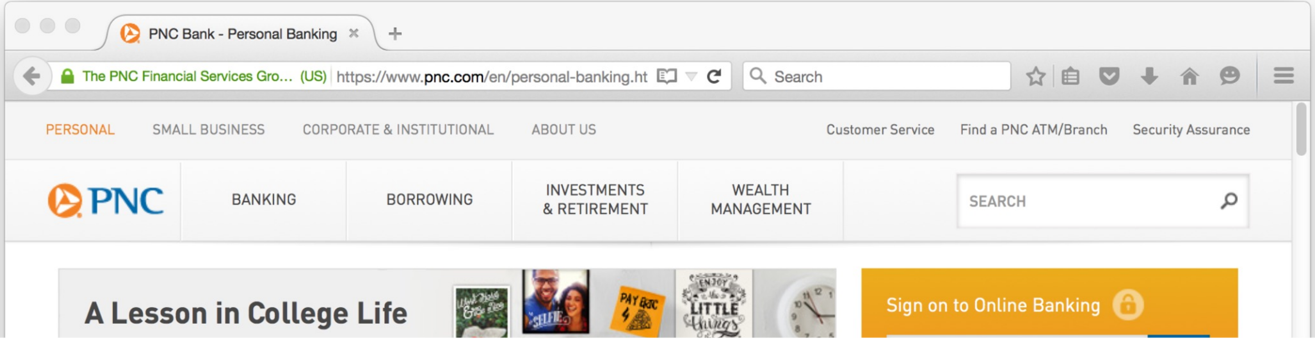
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be cameo.library.cmu.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

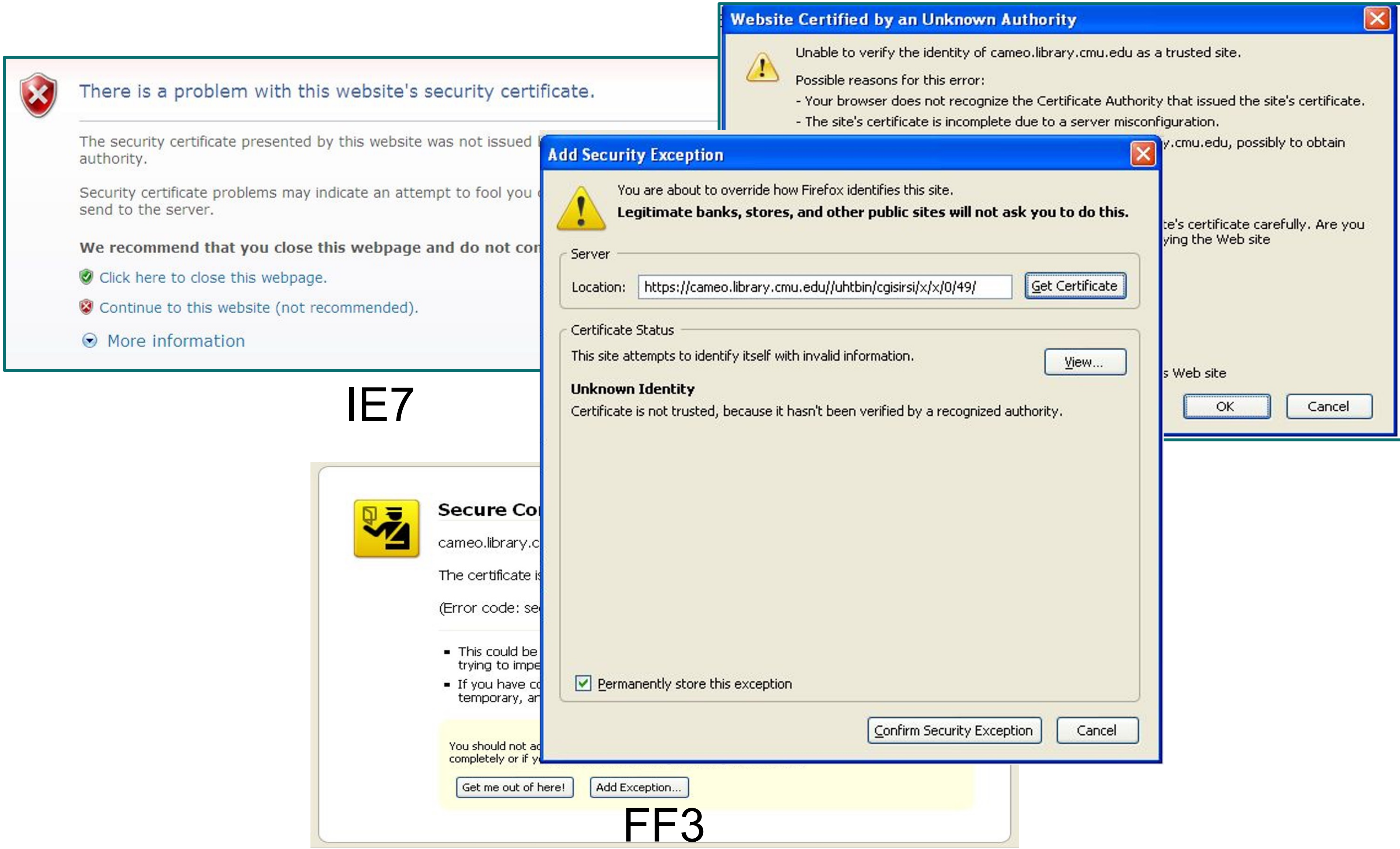
Before accepting this certificate, you should examine this site's certificate carefully. Are you

Risky context

- Put users in situation where they have something they care about at risk
  - Come to our lab and check bank account balance online
- Make users think they are actually at risk
  - ~~Use web proxy to do man-in-the-middle attack~~
  - Delete root certificate from browser so websites trigger warnings



(Then) Existing Warnings



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued
authority.

Security certificate problems may indicate an attempt to fool you
send to the server.

We recommend that you close this webpage and do not co

Click here to close this webpage.
Continue to this website (not recommended).
More information

IE7

Website Certified by an Unknown Authority

Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.

y.cmu.edu, possibly to obtain

te's certificate carefully. Are you
ying the Web site

s Web site

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://cameo.library.cmu.edu//uhtbin/cgisirsi/x/x/0/49/

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Secure Co

cameo.library.c

The certificate i

(Error code: se

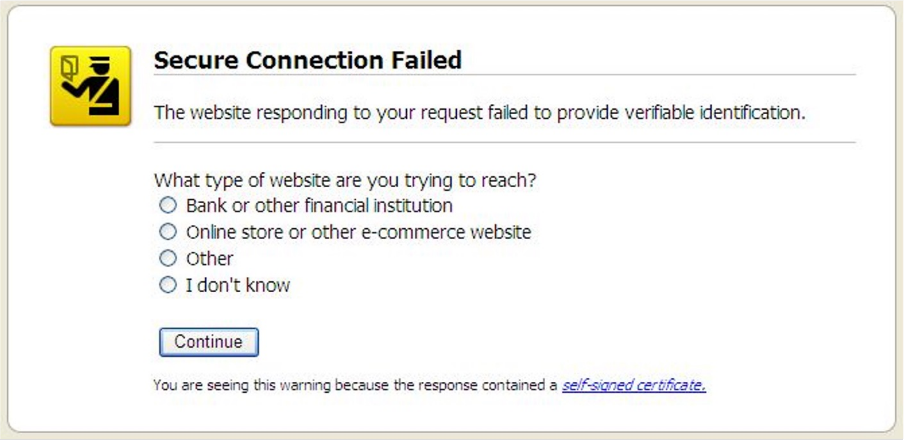
- This could be
trying to impe
- If you have c
temporary, ar

You should not ac
completely or if y

FF3

Additional Possible Warnings

Interactive Warning (Multi-page)



Secure Connection Failed

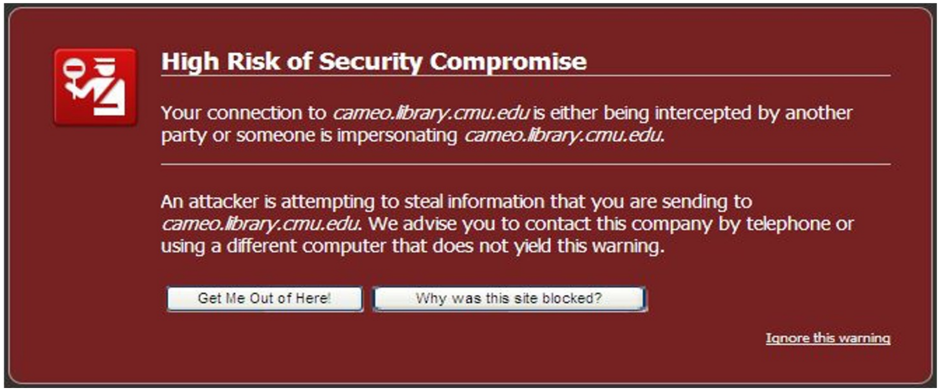
The website responding to your request failed to provide verifiable identification.

What type of website are you trying to reach?

○ Bank or other financial institution
○ Online store or other e-commerce website
○ Other
○ I don't know

You are seeing this warning because the response contained a *self-signed certificate.*

Obvious Warning (Single page)



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu.*

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu.* We advise you to contact this company by telephone or using a different computer that does not yield this warning.

100 participants
In person
Between subjects

Laboratory study tasks

- Users were instructed to find:
  - Total area of Italy using Google
  - Account balance at bank website*
  - Price of *Freakonomics* at Amazon
  - *Richistan* call number with CMU library catalog*

*warning appeared

- Alternate tasks provided
  - Required calling or using a different site
- Post-experiment survey on reactions

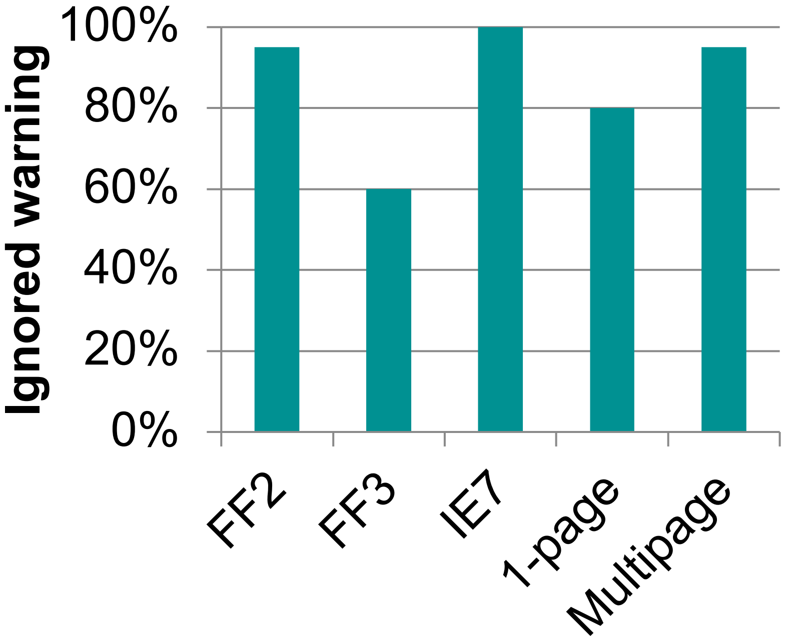
Hypotheses

- Participants would be likely to ignore the IE7 and FF2 warnings on both websites
- Participants would be likely to obey the FF3 and our single-page warning on both websites
- Participants who saw our multi-page warning would obey on bank website, but continue to library website

Library Results

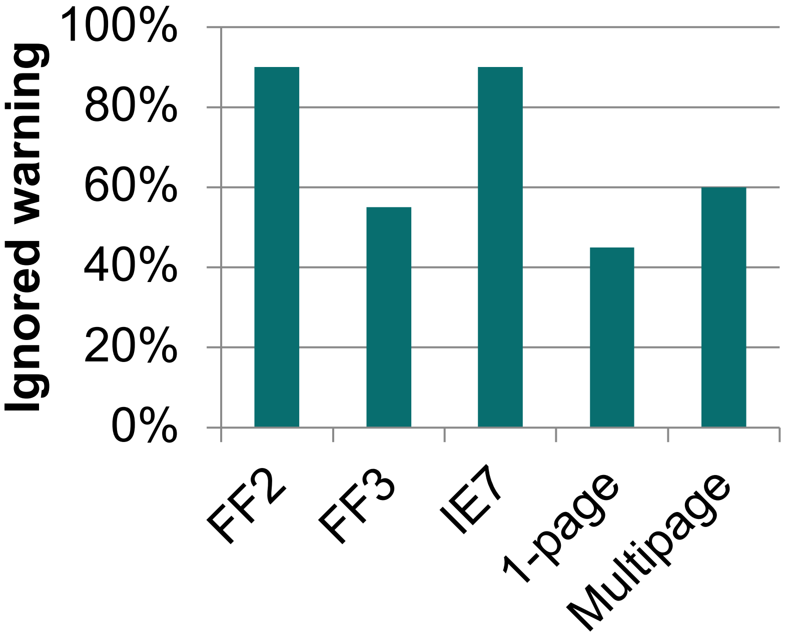
Low-risk (Library)

- More obeyed warning in FF3
- most users ignored warnings in other conditions

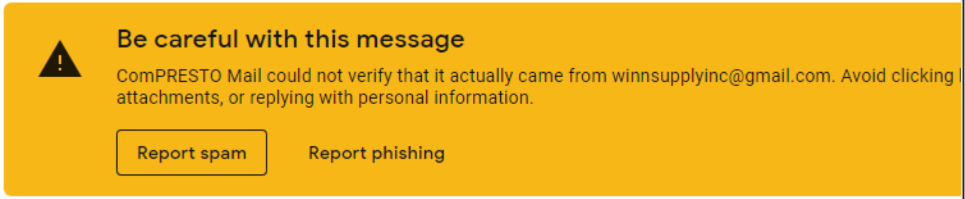


High-risk (Bank)

- More obeyed warning in FF3 and new conditions
- Most ignored in IE7, FF2

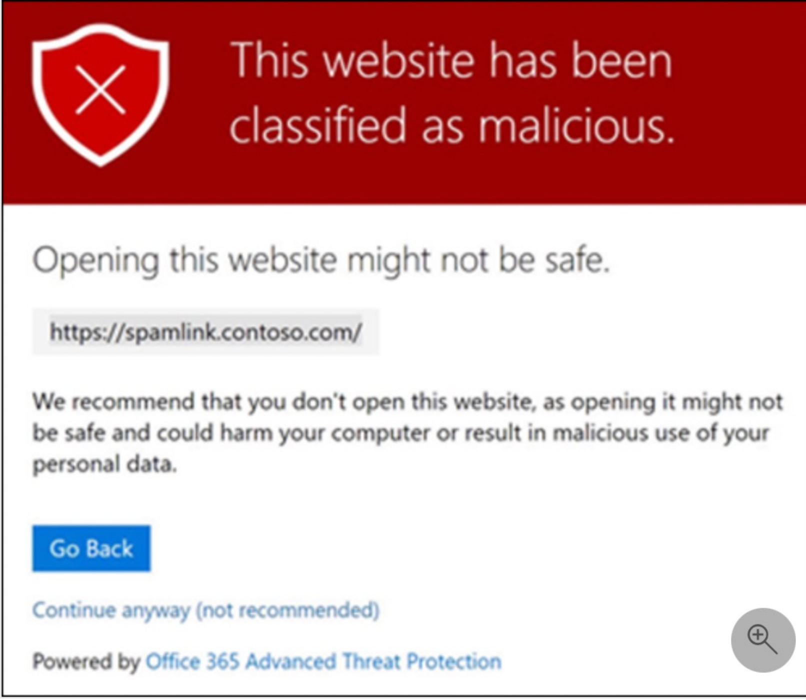


Exercise: Security Exp



Be careful with this message

ComPRESTO Mail could not verify that it actually came from winnsupplyinc@gmail.com. Avoid clicking l attachments, or replying with personal information.



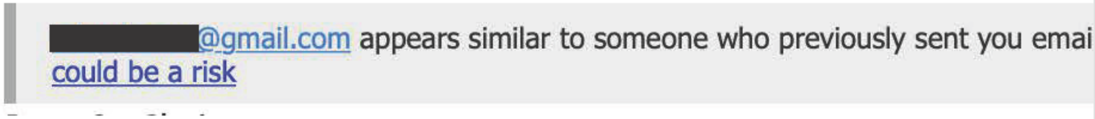
This website has been classified as malicious.

Opening this website might not be safe.

https://spamlink.contoso.com/

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

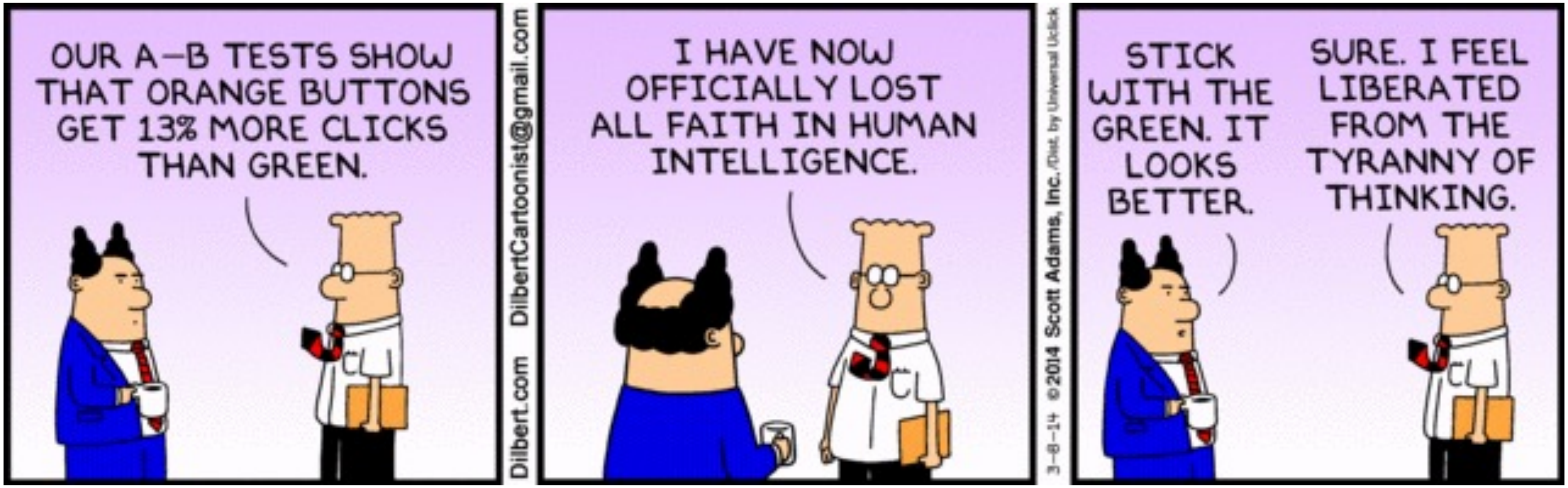
Powered by Office 365 Advanced Threat Protection



[redacted]@gmail.com appears similar to someone who previously sent you emai could be a risk

- Design an experiment that evaluates: What is the most effective way to protect users from phishing attempts?
- Things to consider:
  - What conditions will you have?
  - Within subject or between subject?
  - What tasks will you ask your participants to complete?
  - How will you simulate risk?
  - What data would you collect?
  - Would you conduct this study in person ("lab") or online?

Experiments


OUR A–B TESTS SHOW THAT ORANGE BUTTONS GET 13% MORE CLICKS THAN GREEN.
I HAVE NOW OFFICIALLY LOST ALL FAITH IN HUMAN INTELLIGENCE.
STICK WITH THE GREEN. IT LOOKS BETTER.
SURE. I FEEL LIBERATED FROM THE TYRANNY OF THINKING.

Dilbert.com DilbertCartoonist@gmail.com

3-8-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick