Lecture 5: Experimental User Studies

CS 181W

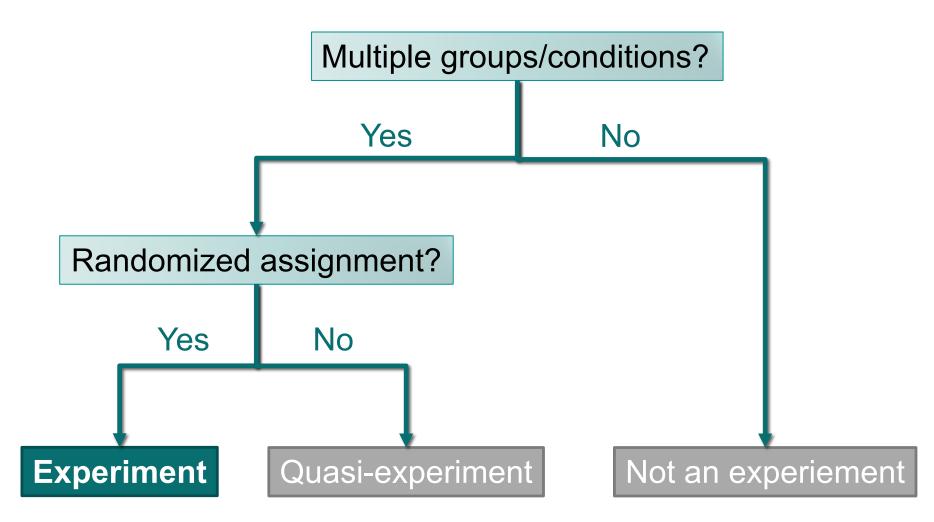
Fall 2022

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?

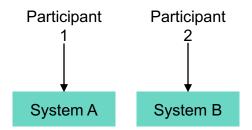
- Observe how people behave in various circumstances
- Test hypotheses about and identify causal relationships
- Can evaluate designs and tools that do not yet exist
- Large-scale experiments (can be) representative of population

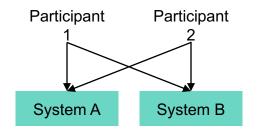
Experimental Study Limitations

- 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)

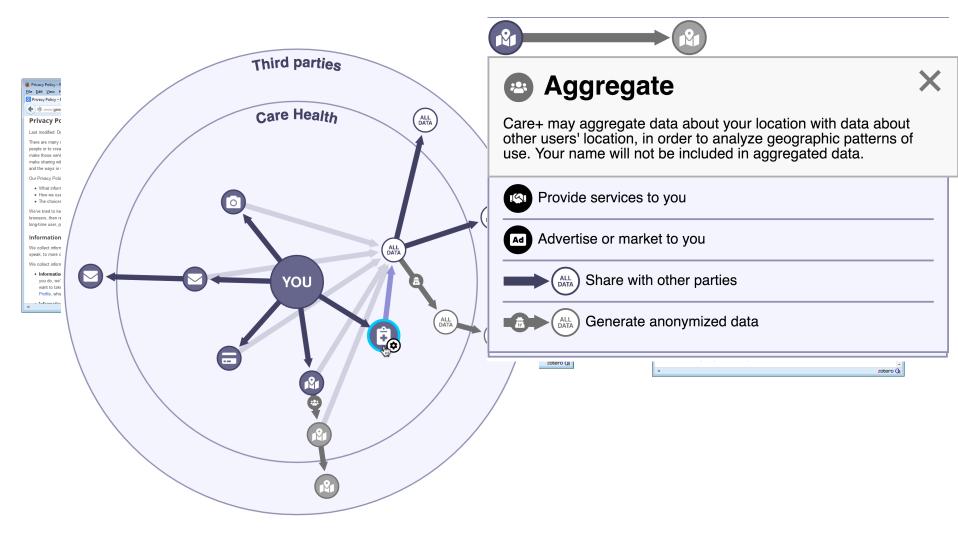




Data to collect during experiments

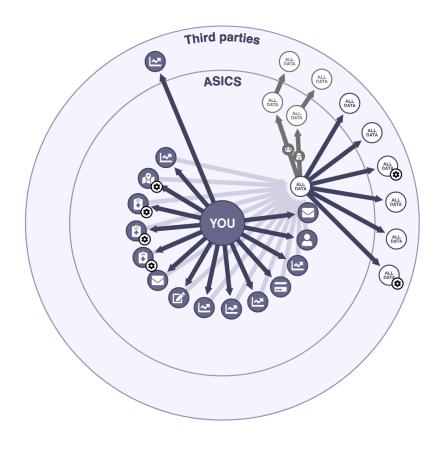
- Performance (time, success rate, errors)
- Actions and decisions
 - Think-aloud, audio, screen capture, video, mouse movements, keystrokes
- Opinions, preferences, and attitudes
- Demographics
 - Age, gender, technical background, income, education, occupation, location, disabilities, first language,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

Example: Usability Experiment



Example: Usability Experiment

Poli-See



Annotated Privacy Policies

USABLEPRIVACY.ORG About Browse Policies

20

1



Reading Level: College (Grade 14)

📢 Feedb

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

Runkeeper runkeeper.com

Privacy Practices (2) Click a category to highlight specific practices automatically identified by

First Party Collection/Use 🕢

User Choice/Control @

Data Retention 🕑

Data Security 🕑

Policy Change 😧

Do Not Track 🕑

Third Party Sharing/Collection @ 10

User Access, Edit and Deletion 🕑 💿

our algorithms

Webpage downloaded 2/17/2019 (current version)

40 privacy statements and 0 choices identified

dentilled

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 identity you, as further described below in 'Personal Data We Collect'.'

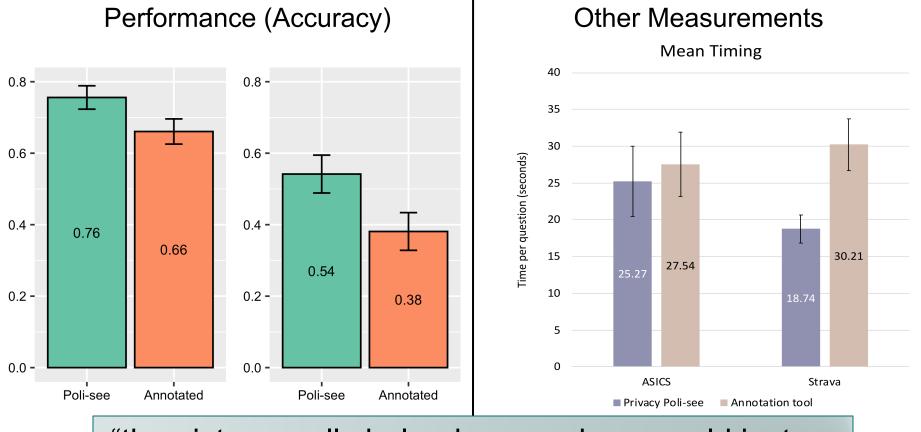
We were unable to automatically locate choices you can make.

Choice Links @

ternational and Specific Audiences 🕑

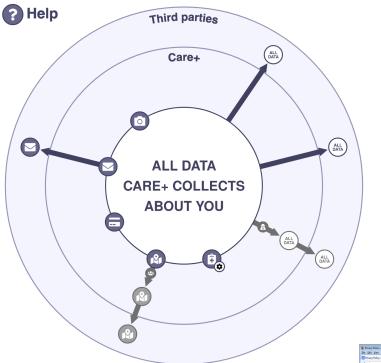
24 participants In-lab Within subject

Example: Usability Experiment



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

Example: Usability Study 2



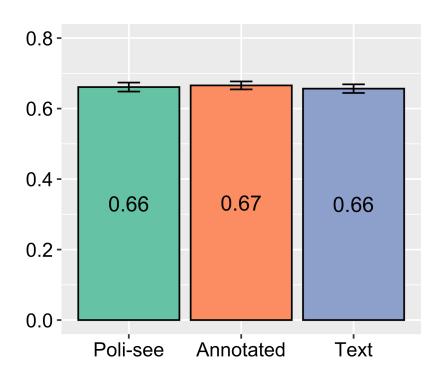
600 participants Online Between subjects

USABLE PRIVACY. ORG 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 Privacy Practices Reading Level: College (Grade 14) Webpage downloaded 2/17/2019 (current version) 40 privacy statements and 0 choices identified Click a category to highlight specific practices automatically identified by our algorithms. First Party Collection/Use @ **Privacy Policy** 20 Third Party Sharing/Collection 🛛 🕕 ASICS PRIVACY POLICY Effective: 25 May 2018 User Choice/Control 😧 2 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 User Access, Edit and Deletion @ that trust. ASICS will take all reasonable steps to protect your information from misuse and keep it Data Retention @ 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. Data Security 🕑 3 SUMMARY Policy Change 😧 • This privacy policy explains the types of personal data we collect and how we use and protect that information: Do Not Track 😧 SCOPE International and Specific Audiences @ 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 Choice Links 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 We were unable to automatically locate through which we can identify you, as further described below in 'Personal Data We Collect'. choices vou can make.

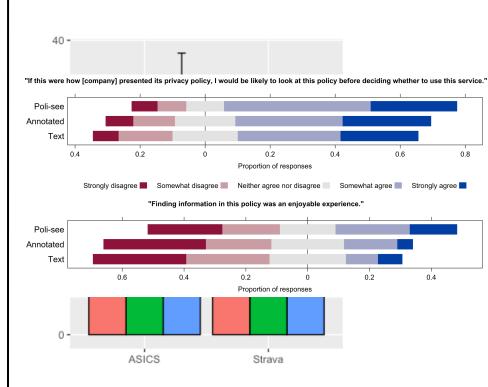
-			🐞 Pelvacy Policy - Policies & Prin						
Privacy Palicy - Policies & Principles - Google - Mazilla Fieldos 🚥 😳 🚾	Elle Edit Yow Higtory Bookmanix Tools Help						🐞 Privacy Policy - Policies & Principles - Geogle - Mozilla Firefex		
Ele Edit Yew Higtory Bookmarks Inois Help			R Privary Deliny - Delicies & Drie	ciples-6 +			Ele Edt Yew Higtory Bookmarks Look Help		
Niney Policy - Policies & Principles - G., +	& Principles - Google - Mos	sila Finefox		and and a second s	<u>⇔</u> ⊽d Q+ ∔ #		Ninacy Policy - Palicies & Principles - G., 4		
🔶 🖲 www.geegle.com/policis/piwe// 🔅 🗸 🔮 🇌	Eeokmarks Icels Help			n access and correction, we will do so for free.			C B www.congle.com/palicies/privacs/	- 	a- i i
Privacy Policy	and the second second			o maintain our services in a manner that protect		1 100			
Privacy Policy		1	0 v d 0 • 4 🔶	er you delete information from our services, we					
Last modified: December 20, 2013 (view archived versions)			HIG ST A		mà.			ect to certain Google products and services that	at you may
There are many different ways you can use our services - to search for and share information, to communicate with other					1		승규리 Q+ 🖡 🛊		
people or to create new content. When you share information with us, for example by creating a Goodle Account, we can	🗸 🔍 🗸 🕹 🚖								a
make those services even better - to show you more relevant search results and ads, to help you connect with people or to			d improve them, to develop new		als outside of Google unless one of the		er trusted businesses or persons to process it for us, based		
make sharing with others quicker and easier. As you use our senices, we want you to be clear how we're using information			red context - like giving you more	승호선 및 - 🖡 🏦	and database to complete the state of the	963	y Policy and any other appropriate confidentiality and security		
and the ways in which you can protect your privacy.									
Our Privacy Policy explains:	usses, pixel tags and	- 合보이 Q+ 🖡 會		ion we callect, so that you can make	1			合 * 여 및 * 🛔 會	
our macy macy expans.	ew to Google or a		fer that require a Google Account.		uals outside of Google when we have		eganizations or individuals outside of Google if we have a	loding physical security measures, to	-
 What information we collect and why we collect it. 	consult this page.		entifies you, we may show them	by using Geogle Dashboard.	sitive personal information.		clasure of the information is reasonably necessary to		
 How we use that information. 		eding numbers, time and	a case you, as ruly a car that	cross the web, such as which				ors and agents who need to know that	
 The choices we affec including how to access and update information. 				etain Google advertising services here.			is or enforceable governmental request. vestigation of potential violations.	sctual confidentiality obligations and may	_
We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies. IP addresses, pixel tags and	thich language you		ry issues you might be facing.	e indeiduals.	sample, for Google Apps users) then		vestigation of potential violations. antiv or technical insules.		
browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a	a you celine.	, browser type, browser	ew about upcoming changes or	1	ganization will have access to your		any or technical issues. Wety of Google, our users or the public as required or		
long-time user, please do take the time to get to know our practices - and if you have any questions consult this page.	a jos come.				rain administrator may be able to:	1 1 2 2	enty or coope, our cases or the public as required or		
			wave your user experience and the	with our services, or to indicate when a	tions you install.	u .		liates, including services offered an other	
Information we collect	Account When		able to have our senices appear	evices may not function properly if your			mation publicly and with our partners – like publishers.	e privacy policies that do not incorporate	
We collect information to provide better services to all of our users - from figuring out basic staff like which language you	redit card. If you	provide about your actual	e or anonymous identifier with	C43.		has	e information publicly to show trends about the general use of		
speak, to more complex things like which ads you'll find most useful or the people who matter most to you online.	blicly visible Google	eologies to determine						viduals, including products or sites that	
		mation on nearby WVF)	sal information, from other Google		clation, legal process or enforceable	60,	we will continue to ensure the confidentiality of any personal	es, or other sites linked from our services	
We collect information in two ways:	rices that you use		at combine DogbleClick cookie	ou share information publicly, it may be		el i	information is transferred or becomes subject to a different	and organizations who advertise our	
· Information you give us. For example, many of our services require you to sign up for a Google Account. When	by and interact with		A CONDINI CONDICICA COORT	rent options on sharing and removing				and offer relevant ads.	
you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you	and methods with				20		-	1	
want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google		about your installation (for	are set out in this Privacy Policy.					1	
Profile, which may include your name and photo.		to Google when you install	d. We may process your personal			1.00	wized access to or unauthorized alteration, disclosure or	everal self regulatory frameworks. When	
- Information on and from concerning of any section. We approved and section about the concerning that approved	m version, unique	h as for automatic updates.		al information. If that information is	zotero	0		emplaint to follow up. We work with the	1
× zotero (sociate your			ave to keep that information for legitimate	We encrypt many of our services using \$35.			easive any complaints regarding the	zotero G
device identifiers or phone number with your Google Account.				a you to verify your identity before we can			our Google Account, and a Safe Browsing feature in Google		
 Log information 		our device using a caches	zntern (Drate		on only score, and one offering where a coope		
		0.000405				and pro-	cessing practices, including physical security measures, to		
When you use our senices or new content provided by Google, we may automatically collect and store			nably repetitive, require dispreportionate technical effort (for example, developing a in existing practice), risk the privacy of others, or would be extremely impractical			zotero (a under this Privacy Policy without your			1
xetain information in source loss. This may include: x moder restrict your and you want you you want you			to existing practice), risk the phacy of others, or would be extremely impactical ratios residing on backup systems). Is and connection, we will do no for thee, eacent where it would remain a.			espect consert. we we post any procey poley changes on was page and, if the changes are significant, we will pr			
					more p		re prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior sions of this Phivacy Policy in an archive for your minew.		
or Gooste Statutes that may appear on other site				zotero (ji					4
к		zotero (j	1		×			zotero G	4

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

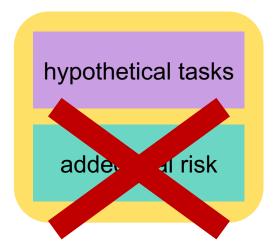


Observing infrequent events and small differences

• 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!



Background: Encryption

Symmetric Encryption

- e.g., AES
- Pros: fast, works on arbitrary-length messages
- Cons: need n² 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







Public key \rightarrow fingerprint

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

mQINBFLsrT0BEADI72WmFPt4Q8+3zhtXfxg7MtIilamR0XLk0CSy5jEJk38rLb6Sxr7TCHD1 sD/W/Iy8atV3UA5MUwTZ12iU08MAGW49qmEp9atY7alFtL2p1mGBV0nd8gx0nuLFstGaFIUv WRV1meRxiU5zneH2S1t+dgjDsUWMN4nFNnP+87FMI98Q82OdwDai7hXtGKaxLYpzIo9gfFGy W2x47FXvMxQTC4pUyavkKsv4Q9qfx4cS/Bxv5eezNn/076b47L/xwJ0gCUJILt4udig7RYyI y8Y0w05cBwVIfd/XzIig7q0vzEgVCLFnhghyJsguLMjRXa/pCuCAiNkeiqHHwdT3GRHSbGh+ SsUJ6JUcj5nzh50DpExEGDv1w1ncE7DIpwpxM+ct4muVMYqhe6moP6rs0a/aTi+3Jw+Hg80n FsKlpizCUsAtTFft94t0FZw+uplu+AGPZ8qD1J490V5GZo+7RkUFYxNq/Zt0GAcB+KaW4MTZ CpDBUJRAnWm/k/n00YbdjQsTR/Si7cnkLFhQMRN3yaETLsE0WKUYBBmJPug7bhkDEWkF15MJ dF1N5EQ7Hb1t1Fi39zYBhZYMkYEaVviRYAP1VQL0CzVSsS4xUyivRsDRmSX7DLmaW8tY1NwE 8QvJ6mjNQy+V/DdSQf9cMdVu7NMnk8Cb5H0uEgj19wywm4wWgQARAQABtB5Kb3NodWEgVGFu IDxqdGFuMTg5QGdtYWlsLmNvbT6JAj0EEwEKACcFAlLsrT0CGwMFCQHhM4AFCwkIBwMFFQoJ CAsFFgIDAQACHgECF4AACgkQiZDZY750wYzPaA//aH6+41N6d1egxPG+NDzcaCPv73gb1xtZ u19fi9WtVAnLBqGyk0HL1Yw+hCH9jFWYfRq8vmiRaRuVQn/7Wf+JcsQway2M7XICeOEg2bPv uR3eQ50jYyvqEkxSgzoBRP46aSm/9S1wHvwp62C5Hu3Cnj1vb/vFQgWB4tfuyVVjqcpn//Qv 0Jas5SZ6TUid6yLpkFq8U1AQo24Wl2Ns8pfXJ0UAfeL0fUoDoQ++0t1V7Zsog7s0IxVXfEyk

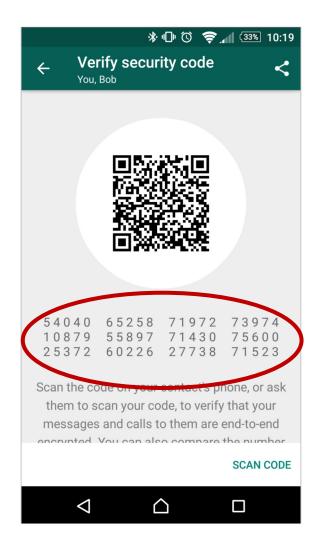
Ke

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

Fingerprint

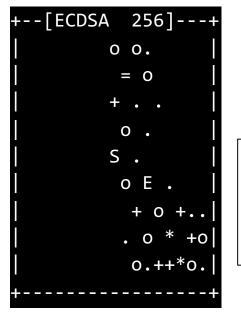
Alice wants to verify Bob's fingerprint

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



What type of fingerprint is best?

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



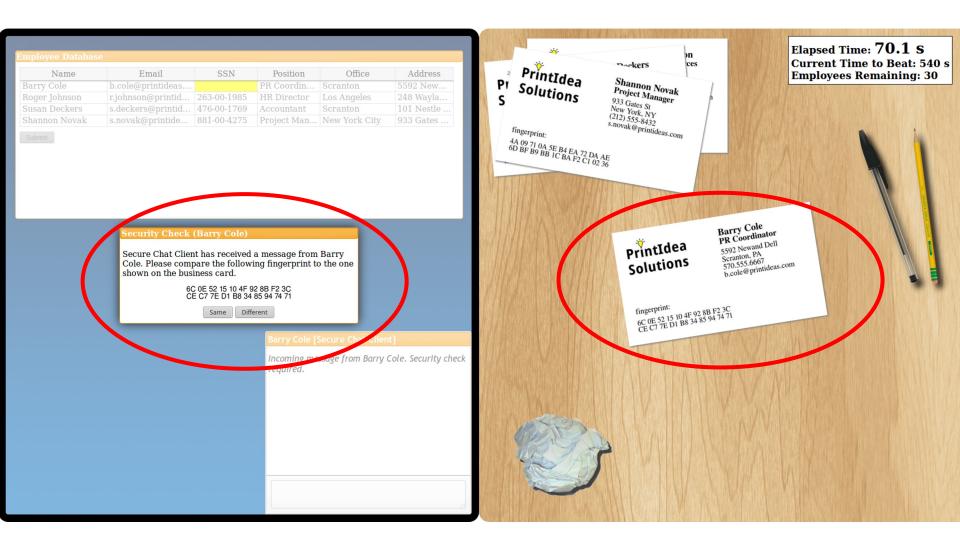
tin yellow blood short attention tax danger bulb wood the normal healthy up false nut bright

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



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!



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

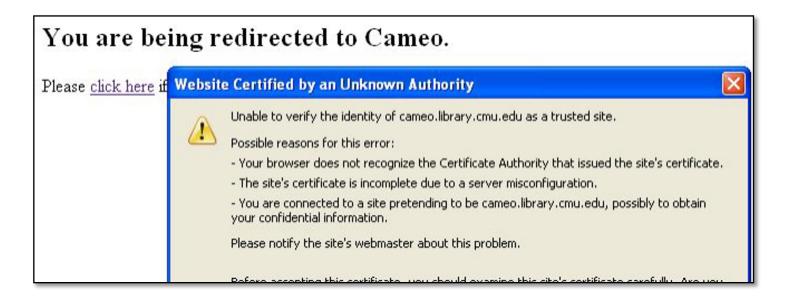
- Browsers warn about SSL Cert problems:
 - Domain Mismatch
 - Unknown Certificate Authority
 - Expired
- These warnings
 - May be user's only protection
 - Commonly encountered when connecting to legitimate servers

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

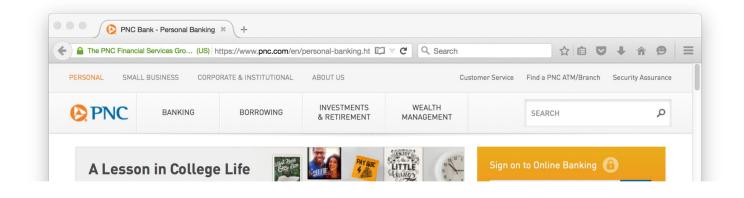
Non-risky context

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



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

		Website Certified by an Unknown Authority	
8	There is a problem with this website's security certificate.	Unable to verify the identity of cameo.library.cmu.edu as Possible reasons for this error: - Your browser does not recognize the Certificate Authorit - The site's certificate is incomplete due to a server miscon	y that issued the site's certificate.
	The security certificate presented by this website was not issued Add Security Exce	eption 🛛	y.cmu.edu, possibly to obtain
	becancy conditioned problems may indicate an accompt to roor you	out to override how Firefox identifies this site. :e banks, stores, and other public sites will not ask you to do this.	:e's certificate carefully. Are you ving the Web site
	We recommend that you close this webpage and do not con		ying the web site
	Click here to close this webpage.	//cameo.library.cmu.edu//uhtbin/cgisirsi/x/x/0/49/	
	Sontinue to this website (not recommended).	Remainment	
		to identify itself with invalid information. <u>View</u>	s Web site
	Secure Co cameo.library.c The certificate it (Error code: se • This could be trying to impe • If you have co • Thy could not ac Completely or if y Get me out of here! Add Exception	tore this exception Cancel	

Additional Possible Warnings

Interactive Warning (Multi-page)

Obvious Warning (Single 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
- O Other
- I don't know



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



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.

Why was this site blocked?

Get Me Out of Here!

Ignore 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



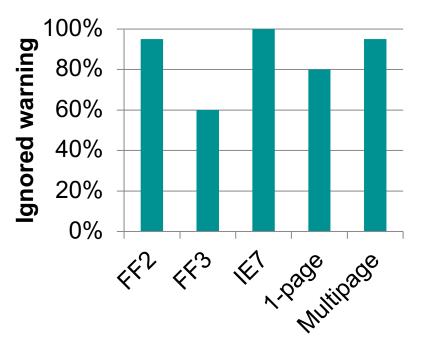
Hypotheses

- 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

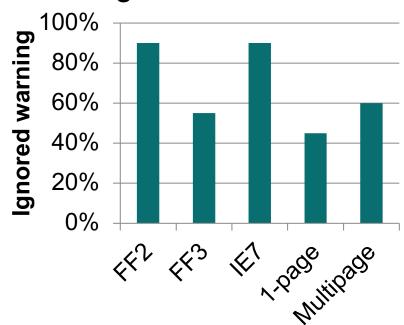
Low-risk (Library)

- 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





This website has been classified as malicious.

Exercise: Security Exp

ComPRESTO Mail could not verify that it actually came from winnsupplyinc@gmail.com. Avoid clicking

Ogmail.com appears similar to someone who previously sent you email

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.

Go Back

Continue anyway (not recommended)

Powered by Office 365 Advanced Threat Protection

- Design an experiment that evaluates: What is the most effective way to protect users from phishing attempts?
- Things to consider:

Be careful with this message

Report spam

attachments, or replying with personal information.

Report phishing

A

could be a risk

- 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?

Ð

Experiments

