01- Course overview and introductions

Lorrie Cranor

January 18, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today's class

- Course staff introductions
- Usable security and privacy = ???
- Overview of course topics
- Course policies / syllabus
- Student introductions

Introductions

- Lorrie Cranor
- Professor of Computer Science and Engineering & Public Policy
- Director, CyLab Usable Privacy and Security Laboratory
- Co-director, MSIT-Privacy Engineering
- Used to work for AT&T Labs and FTC
- Office hours: by appointment

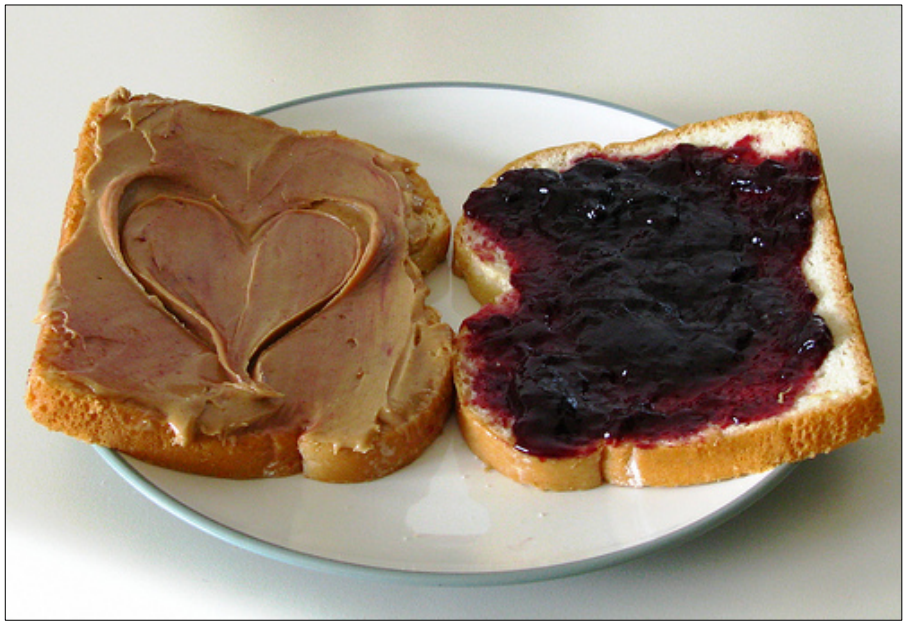
Humans

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations… But they are sufficiently pervasive that we must design our protocols around their limitations."

— C. Kaufman, R. Perlman, and M. Speciner.
Network Security: PRIVATE Communication in a PUBLIC World.
2nd edition. Prentice Hall, page 237, 2002.

Better together

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



Interdisciplinary approach useful

Other disciplines have experience studying human behavior. We can borrow their models and methods:

- Psychology
- Sociology
- Ethnography
- Cognitive sciences
- Warnings science
- Risk perception
- Organizational change
- Behavioral economics
- HCI
- Marketing
- Counterterrorism
- Communication
- Persuasive technology
- Learning science
- Network analytics

What makes usable security different?

- Presence of an adversary
- Usability is not enough. We also need systems that remain secure when:
  - Attackers (try to) fool users
  - Users behave in predictable ways
  - Users are acting under stress
  - Users are careless, unmotivated, busy

Usable security research bridges security and usability

Security	Usability/HCI	Usable Security
Humans are a secondary constraint to security constraints	Humans are the primary constraint, security rarely considered	Human factors and security are both primary constraints

Usable security research bridges security and usability

Security	Usability/HCI	Usable Security
Humans are a secondary constraint to security constraints	Humans are the primary constraint, security rarely considered	Human factors and security are both primary constraints
Humans considered primarily in their role as adversaries/attackers	Concerned about human error but not human attackers	Concerned about both normal users and adversaries
Involves threat models	Involves task models, mental models, cognitive models	Involves threat models AND task models, mental models, etc.
Focus on security metrics	Focus on usability metrics	Considers usability and security metrics together
User studies rarely done	User studies common	User studies common, often involve deception + active adversary

User-selected graphical passwords

Security	Usability/HCI	Usable Security

User-selected graphical passwords

Security	Usability/HCI	Usable Security
What is the space of possible passwords? How can we make the password space larger to make the password harder to guess? How are the stored passwords secured? Can an **attacker** gain knowledge by observing a user entering her password?	How *difficult* is it for a **user** to create, remember, and enter a graphical password? How long does it take? How hard is it for users to learn the system? Are users *motivated* to put in effort to create good passwords? Is the system *accessible* using a variety of devices, for users with disabilities?	All the security/privacy and usability HCI questions How do **users** select graphical passwords? How can we help them choose passwords harder for **attackers** to predict? As the password space increases, what are the impacts on usability factors and predictability of human selection?

Goals for this course

- Gain an appreciation for the importance of usability within security and privacy
- Learn about current research in usable privacy and security
- Learn how to conduct usability studies
- Learn how to critically examine UPS studies you hear about or read about

Policies and logistics

- Updated syllabus is always available:
  http://cups.cs.cmu.edu/courses/ups-sp17/

Which course #?

- Ph.D. students must take 12-unit version
- Undergrads: 9-unit version
- Master's students: check with your program
- If you switch sections, you will be waitlisted (but we will let you in)

Components of your grade

- Homework: 30%
- Quizzes: 20%
- Midterms: 20%
- Class Project: 30%

Readings

- Generally one required reading per class
  - There will be quizzes – see next slide
- Complete the readings before class
- Textbook: Lazar et al.'s *Research Methods in Human-Computer Interaction*
  - Available as an ebook from CMU library
- Most readings from recent conferences
- 12-unit students: one additional reading for most classes (see homework)

Quizzes

- Given in the first five minutes of class
  - End at 3:05 pm
- Will be a quick quiz based on that day's required reading
- If you will be unable to arrive on time for a class, submit a reading summary and highlight of the required readings before class

Homework

- 10 homework assignments
  - Drop single lowest grade
  - No late homework accepted!
- For 12-unit students
  - These will usually include a “reading summary” of one optional reading per class
  - 3-7 sentence summary
  - One “highlight”

What is the homework like?

- Conduct mini studies + report results
- Evaluate the incidence or state of something in the real world
- Conduct usability evaluations of tools
- Propose possible studies
- Other activities

Homework 1 is already posted (and due Jan 30)!

Example reading summary

Ur et al. investigated whether crowdsourced recommendations impact the Firefox privacy settings humans and sloths choose. They conducted a 183-participant lab study in which participants were prompted to set up a clean installation of Firefox as they normally would when given a new computer. Participants were randomly selected either to see crowdsourced recommendations for the settings, or no recommendations. They found that both humans and sloths were statistically significantly more likely to choose privacy-protective settings when given recommendations, though sloths took 83 times as long to do so.

Highlight: I wonder if the results would have differed if they had used Chrome, rather than Firefox. Chrome's privacy settings are hidden behind multiple browser clicks. I would be surprised if Chrome recommendations change non-use of privacy settings.

Midterms (two of them)

- Given about one-third and two-thirds of the way through the class
- 20% of your grade
- These will ask you to use the skills developed in class, rather than remembering trivia
- Prepare by doing the readings and participating in discussions

Project

- Design, conduct, and analyze a user study in usable privacy or security
  - Groups assigned based on your preferences
  - We will provide a list of project topics but your suggestions are welcome
- Deliverables: Project proposal, IRB application, progress report & presentation, final paper, and a final presentation (on last day of class)
- Submit a poster to SOUPS 2017 and/or a paper to another conference

Projects from prior UPS courses

- The Post that Wasn't: Exploring Self-Censorship on Facebook (CSCW ‘13)
- How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation (USENIX Security ‘12)
- QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks (USEC ‘13)
- Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption" (USEC '15)
- Supporting Privacy-Conscious App Update Decisions with User Reviews (SPSM ‘15)
- Usability and Security of Text Passwords on Mobile Devices (CHI ‘16)

Participation in class

- You are expected to participate in class
  - Raise your hand during discussions
  - Share interesting privacy/security news
  - Play an active role in small-group activities
  - Spark discussion on the class email list
- You are expected to be in class (on time!)
- Please note exam and group presentation dates and DO NOT schedule job interviews on those dates

Academic integrity

- Make yourself familiar with CMU's policies about plagiarism and academic integrity
- Don't even look at other students' homework assignments
  - Exception: When we explicitly say that you may work in groups for a particular task
- Quote text and cite ideas that are not yours
- Consequences of cheating and plagiarism range from a 0 on the assignment to expulsion from CMU

More logistics

- There is no final exam
- We have no Blackboard site
- We will sign you up for a course e-mail list
- You may wish to join the CUPS mailing list
  - Weekly CUPS/privacy lunch seminar (Thursdays@ Noon)
  - News and opportunities of interest
  - To sign up, follow link on course webpage

Course topics

- Introduction to HCI methods and the design of experiments
  - How (and why) to conduct different types of quantitative and qualitative studies
  - Ecological validity and ethics
  - Overview of statistics
- Quick overviews of security and privacy
- Specific usable privacy and security topics

Topic: Passwords

- At least 8-characters.

- Can people make passwords that are easy to remember, yet hard to crack?

Password strength: Poor. Consider adding a digit or making your password longer.

hashcat
advanced
password
recovery

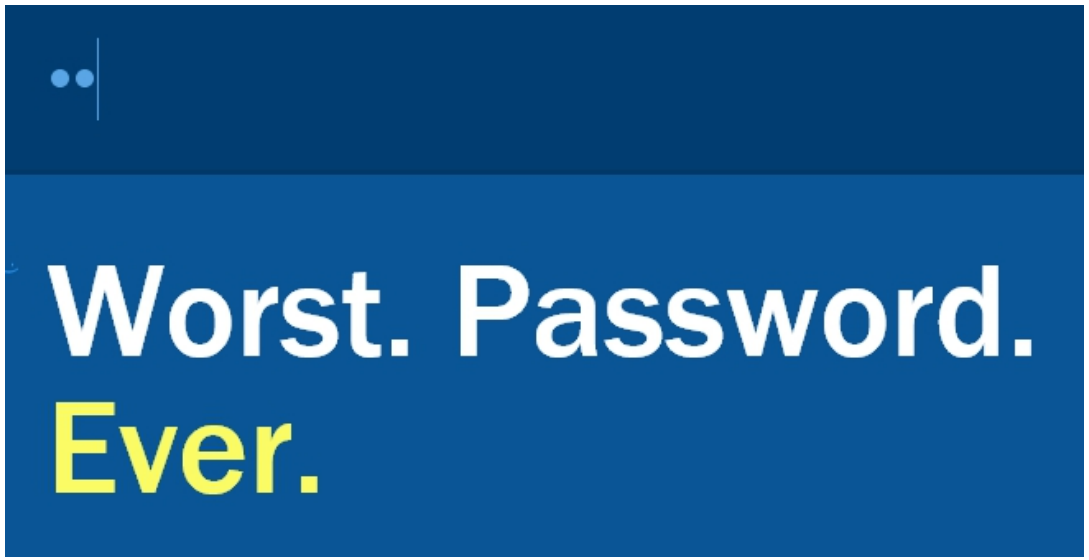


Image from http://www.trypap.com

Topic: Secondary authentication

- Mother's maiden name?
- Favorite athlete?
- A code sent to your phone?

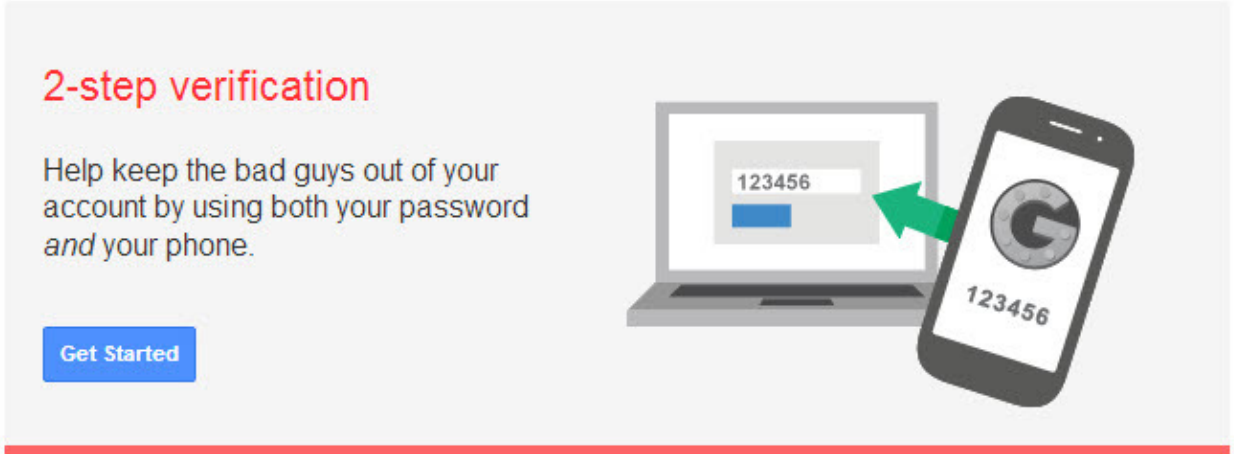


Image from http://www.wikipedia.org

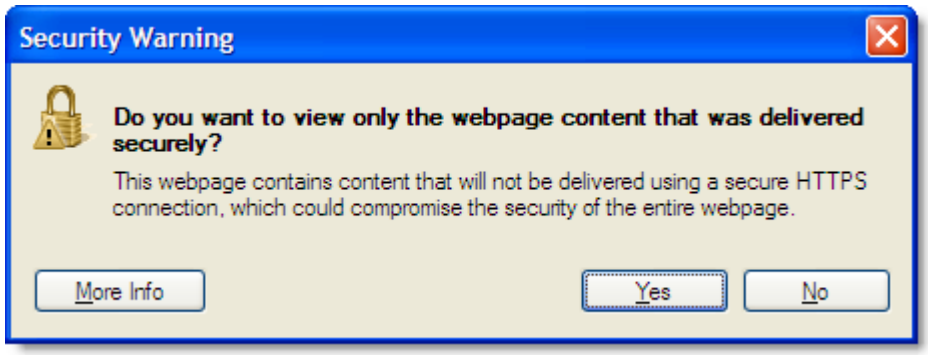
Topic: Privacy Tools

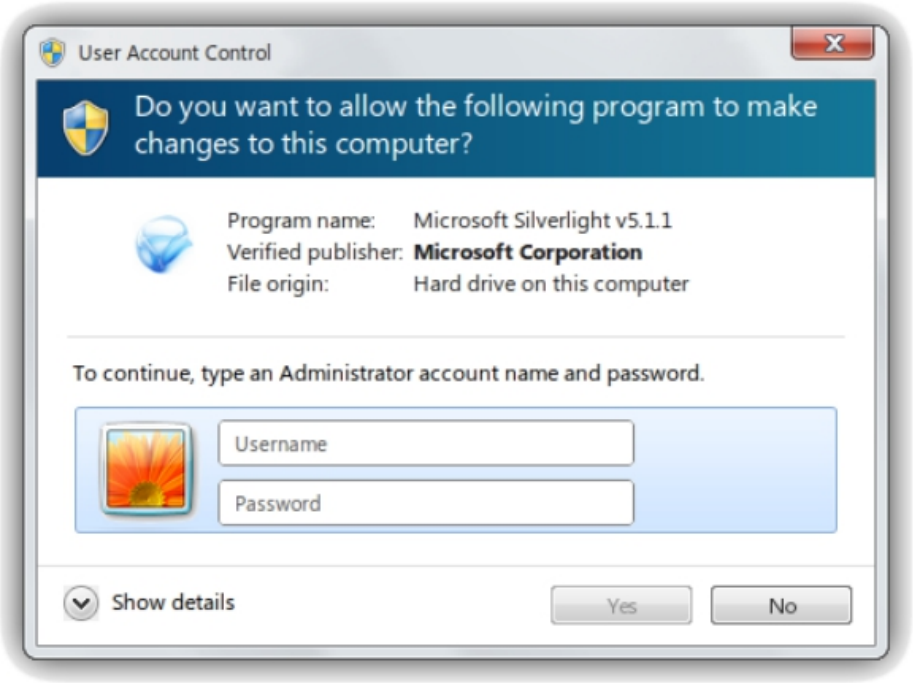
- How can tools help users protect their privacy?
- How usable are those tools?

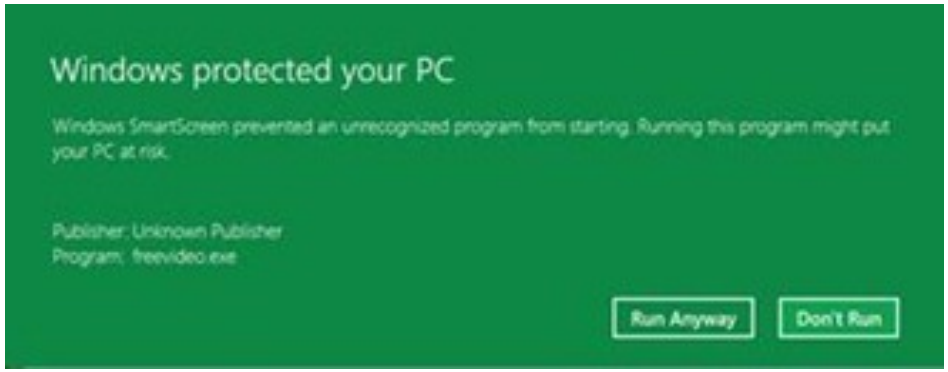
Image from http://www.wikipedia.org

Topic: Security warnings

- Can we make them more effective?







Topic: Smartphones and UPS

- Do people understand where the information on their phone goes?
- …And can someone please make app permissions usable?

Image from http://www.nokia.com

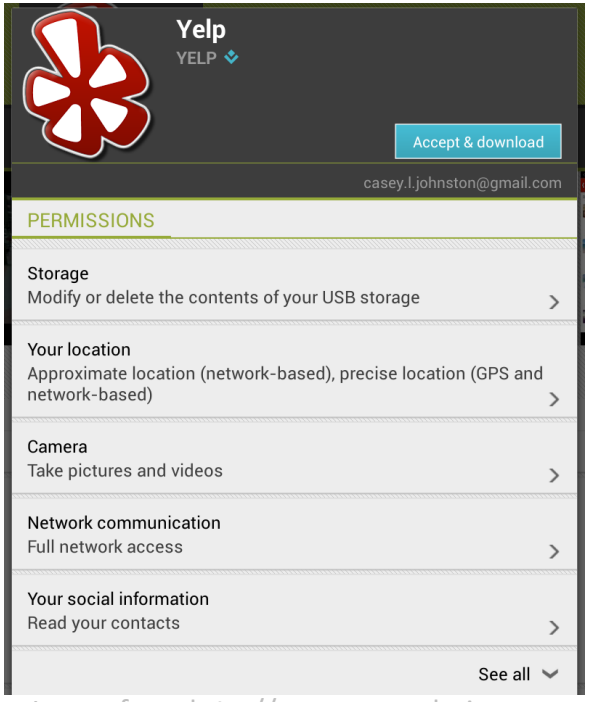


Image from http://www.arstechnica.com

Topic: Mobile and UbiComp

- What are the privacy and security implications of devices that go wherever you go?
- How can that be addressed?

Topic: Privacy policies and notices

- How do we communicate privacy-critical information in a sea of information?

SoundCloud **Class B**

- You stay in control of your copyright
- Collected personal data used for limited purposes
- 6 weeks to review changes
- Indemnification from claims related to your content or your account
- Personal information can be disclosed in case of business transfer or insolvency

More details

Screenshot from http://www.tosdr.org

Rev. 12/2010

FACTS WHAT DOES **FARMERS-MERCHANTS BANK (FM Bank)** DO WITH YOUR PERSONAL INFORMATION?

Why? Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What? The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and **Income**
- **Account balances** and **Payment History**
- **Credit history** and **Credit scores**

When you are *no longer* our customer, we continue to share your information as described in this notice.

How? All financial companies need to share **customer's** personal information to run their everyday business. In the section below, we list the reasons financial companies can share their

Amazon Privacy Policy

types of information	how we use your information: provide service & maintain site	research & revelopment	marketing	telemarketing	profiling	who we share your information with: other companies	public forums
contact information			opt out	opt out		opt in	
cookies			opt out	opt out		opt in	
demographic information							
financial information							
health information							
preferences			opt out	opt out		opt in	
purchasing information			opt out	opt out		opt in	
social security number & govt ID							
your activity on this site			opt out	opt out		opt in	
your exact location							

we **will** collect and use your information in this way

opt out — by default, we **will** collect and use your information in this way unless you tell us not to by opting out

we **will not** collect and use your information in this way

opt in — by default, **we will not** collect and use your information in this way unless you allow us to by opting in

Topic: Biometrics

- Characteristics of the human body can be used to identify or authenticate
  - How can this be done in a user-friendly way?

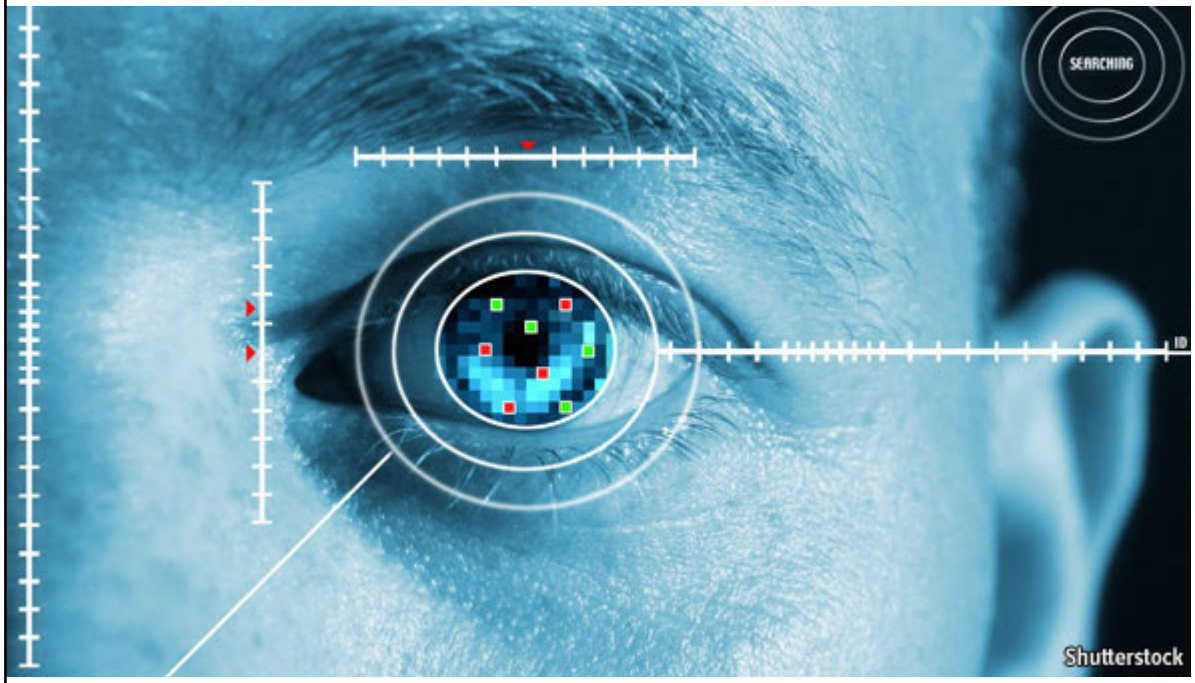


Image from http://www.economist.com

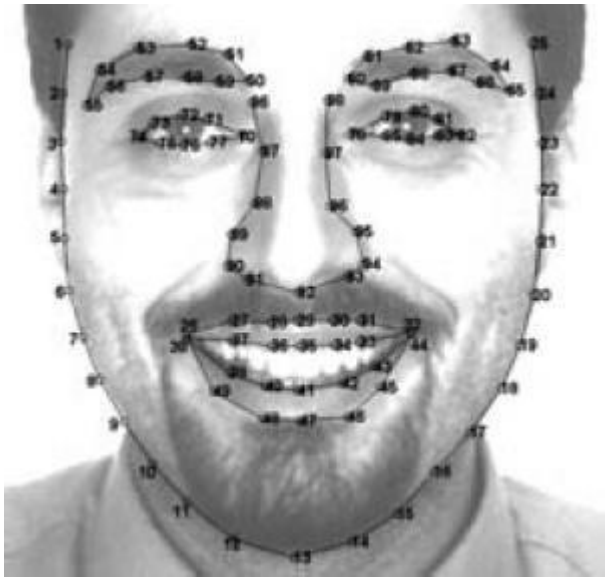
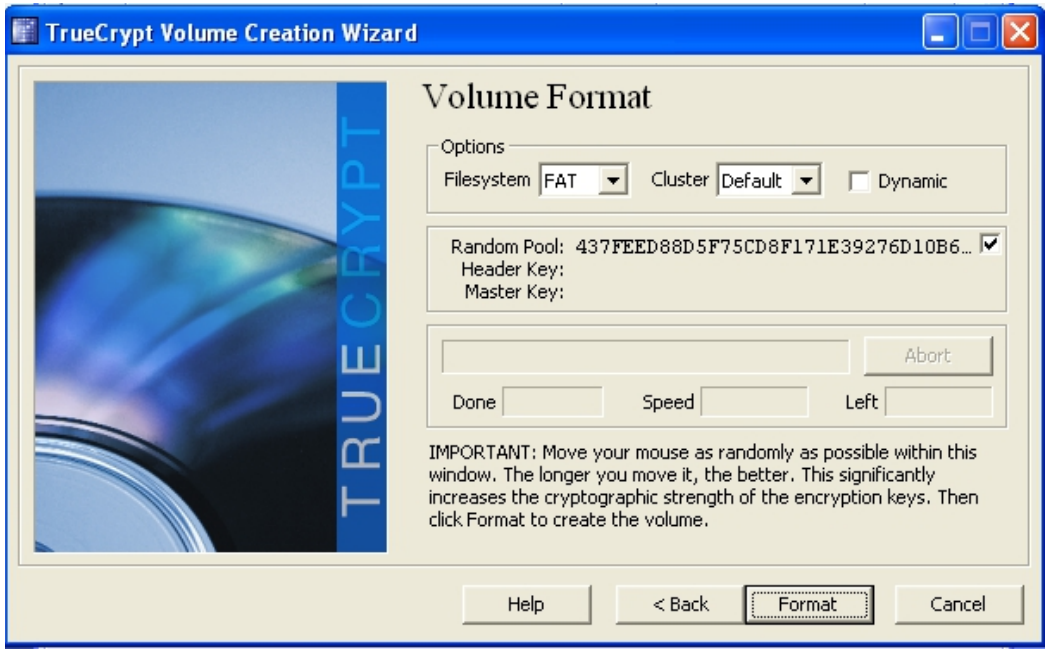
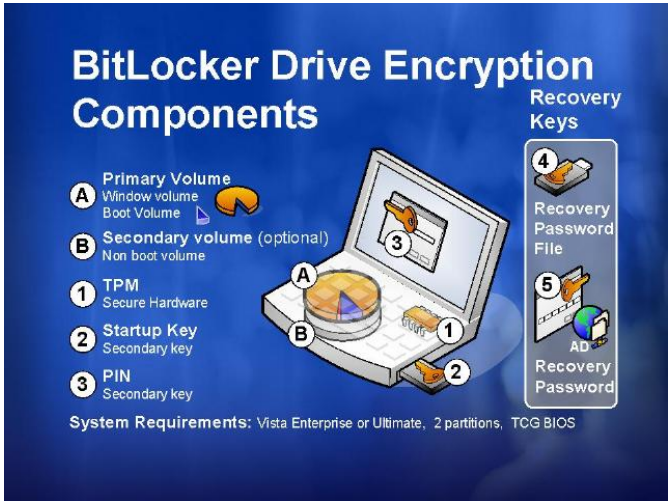


Image from http://www.sciencedaily.com

Topic: Usable encryption

- Why don't people encrypt their email and their files?

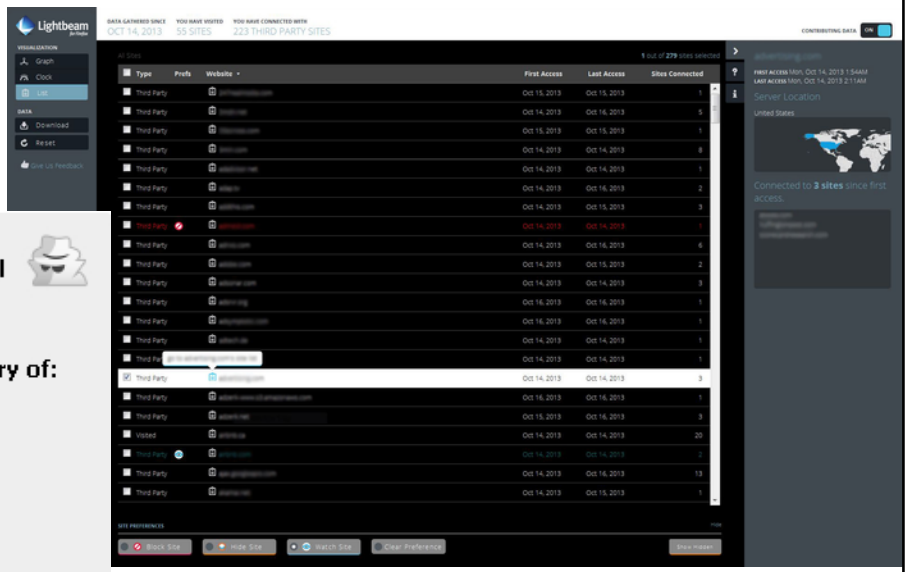




Topic: Browser privacy & security

- What kinds of tracking currently occurs, and what do average people think of it?
- … And why has phishing been so effective?

AdChoices



You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close **all** open incognito windows. Any files you download or bookmarks you create will be preserved, however.

Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:

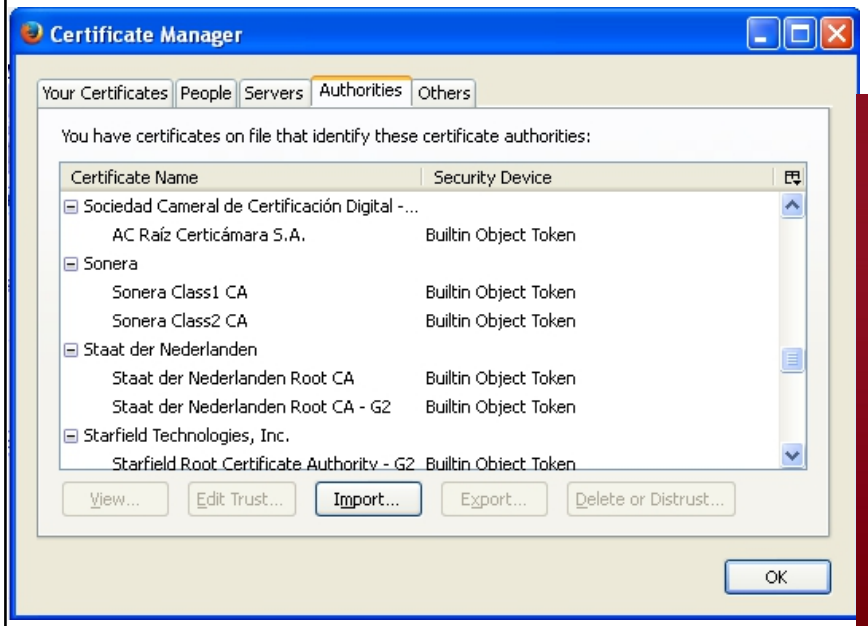
- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

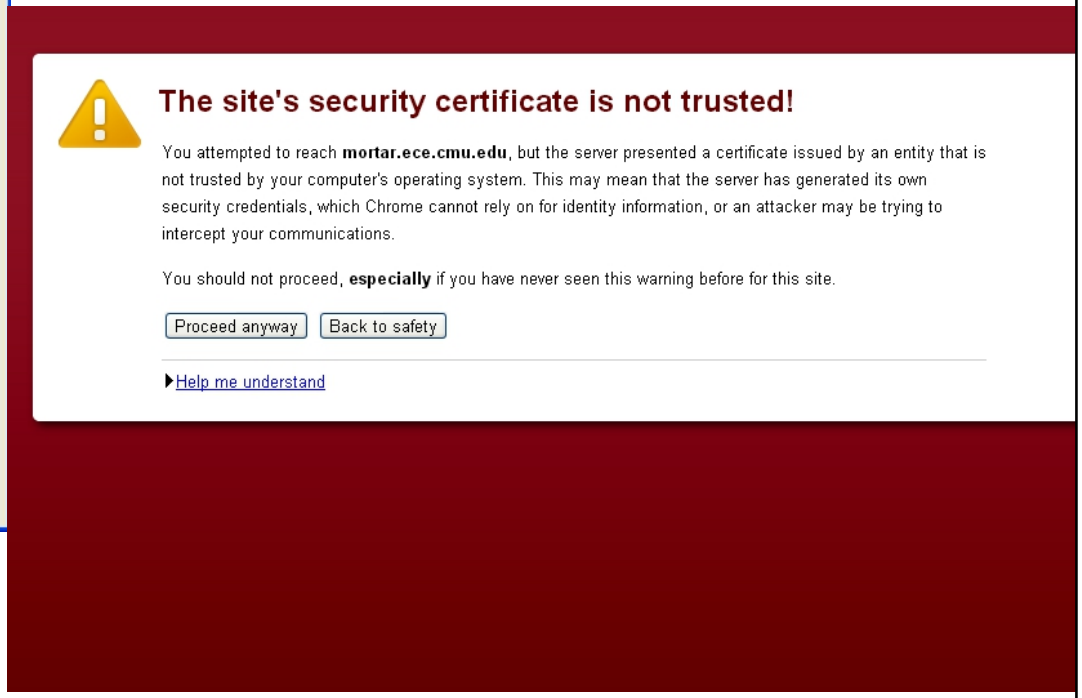
Learn more about incognito browsing.

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can reenable them individually in the extensions manager.

Topic: SSL and PKIs

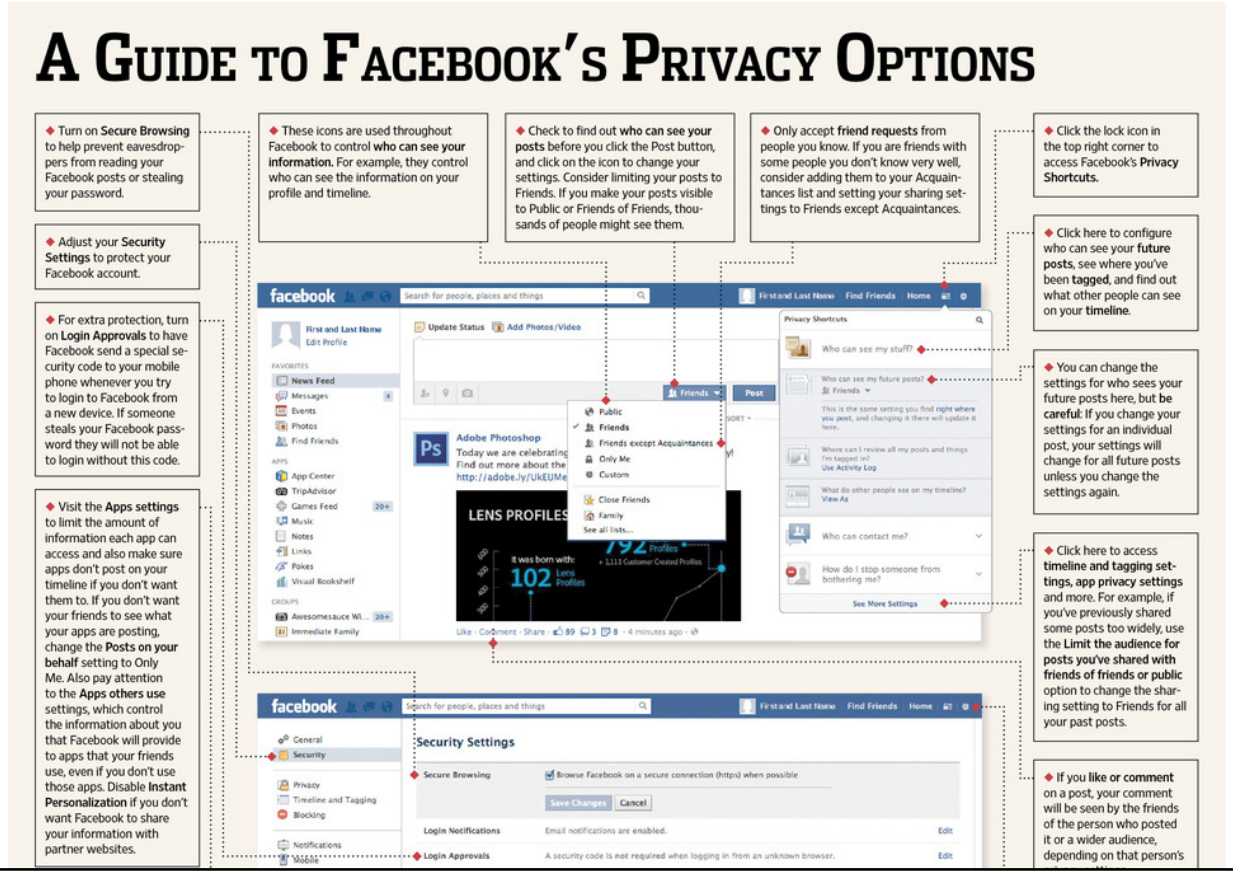
- Is there any hope for making certificates and SSL warnings usable?

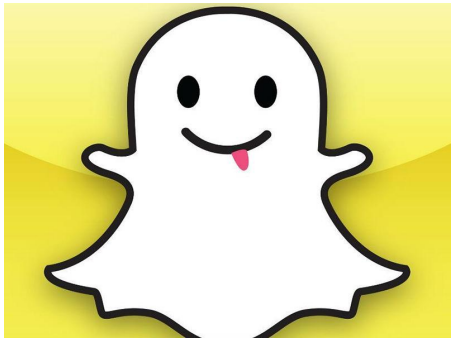




Topic: Social networks and privacy

- Can people want to share some things widely yet want other things to be private?





Topic: Mental models

- How do average people think about privacy and security, and how can we help them and educate them?

Image from http://www.quickmeme.com

Topic: UPS in safety-critical devices

- Some cars, medical devices, and household appliances contain computers
  - How do we help users protect their privacy and maintain security while still reaping the benefits of these new technologies?

Image from http://www.motortrend.com

Image from http://www.hcwreview.com

Image from http://www.allaboutsymbian.com

Topic: Usable access control

- Controlling who has access to your files, physical spaces, and online posts is hard

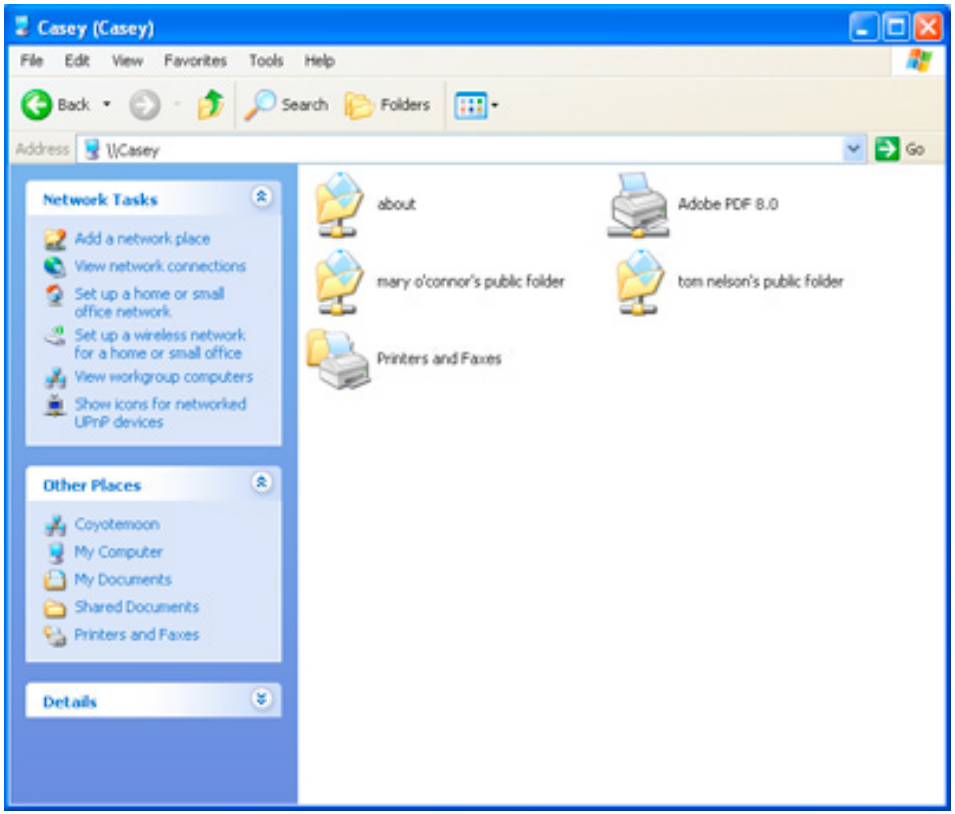


Image from http://www.about.com

Topic: User education

- How can we encourage (*nudge*) people to think about privacy and security?

wombat security technologies

Who you are?

- Your preferred name
- Program at CMU (e.g., Privacy Engineering, COS, ECE, Master's in HCI)
- Why did you sign up for this course?
- Your first (ungraded) quiz